VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Demonstrace kryptografických algoritmů

Demonstration of Cryphtographic Algorithms

2015 Jiří Vávra

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání bakalářské práce

Student: **Jiří Vávra**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R025 Informatika a výpočetní technika

Téma: Demonstrace kryptografických algoritmů
Demonstration of Cryphtographic Algorithms

Zásady pro vypracování:

Cílem práce vytvořit aplikaci pro demonstraci vybraných kryptografických algoritmů.

Práce bude obsahovat tyto části:
1. Stručnou historii kryptografie, kryptologie (důvody vzniku, historické souvislosti, ukázky použití...).
2. Stručný popis vybraných šifrovacích algoritmů - Caesarova šifra, polyalfabetické šifry, Enigma.
3. Implementaci demonstrační aplikace.
4. Implementaci a demonstraci základů kryptoanalýzy vybraných šifrovacích algoritmů.

Seznam doporučené odborné literatury:

Podle pokynů vedoucího bakalářské práce.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **doc. Mgr. Jiří Dvorský, Ph.D.**

Datum zadání: 01.09.2013

Datum odevzdání: 07.05.2015

doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 7. května 2015 .....

Rád bych poděkoval panu doc. Mgr. Jiřímu Dvorskému, Ph.D. za odborné vedení této bakalářské práce, za cenné rady, připomínky a za věnovaný čas. Také bych rád poděkoval své rodině a přítelkyni za trpělivost a podporu při mém studiu.

Abstrakt

Cílem této práce je seznámit čtenáře se základními druhy kryptografických a kryptoanalytických algoritmů spolu s historií kryptologie. V teoretické části jsem ukázal fungování vybraných algoritmů a popsal historii kryptologie. Praktická část je program, kde jsou implementovány algoritmy z teoretické části a uživatel si může vyzkoušet jejich funkci. Výsledkem této práce je poučení čtenáře o základech kryptologie a vytvoření programu k praktické ukázce.

Klíčová slova: šifrování, dešifrování, kryptografie, šifra, enigma, vigener, caesar

Abstract

The purpose of this work is to introduce basic types of cryptographic and cryptanalysis algorithms along with history of cryptology. In theoretical part, I showed the functioning of selected algorithms and describe history of cryptology. The practical part is program, where are implemented algorithms from practical part and user can test their function. The result of this work is to enlighten reader about basics of cryptology and create aplication for practical demonstration.

Keywords: encrypt, decrypt, cryptography, cipher, enigma, vigener, caesar

Seznam použitých zkratek a symbolů

AES	–	Advanced Encription Standard
ARPA	–	Advanced Research Projects Agency
ASCII	–	American Standard Code for Information Interchange
DES	–	Data Encription Standard
GCHQ	–	Governement Communication Headquaters
NSA	–	National Security Agency
PGP	–	Pretty Good Privacy
RSA	–	iniciály autorů Rivest, Shamir, Adleman
WEP	–	Wired Equivalency Privacy
WPA	–	Wi-Fi Protected Access

Obsah

Seznam obrázků

Seznam výpisů zdrojového kódu

1 Úvod

Šifrování a s tím spojené ukrývání dat je v historii lidstva velice důležité. Často záleží na schopnosti vědět nebo nevědět nějakou informaci. Tato schopnost rozhoduje o věcech obyčejných, jako je třeba dětská hra, přes vážnější, což může být odhalení milence, až k takovým, které rozhodují o rozdělení moci ve společnosti nebo o životě a smrti mnoha lidí. Tím se z kryptologie stává velice důležitá nauka. Aktuálně, s rozšířením internetu, který využíváme třeba k online nakupování, bankovnictví a organizaci našeho život, je tento obor state aktuální. To je také důvod k výběru tohoto téma. Dalším důvodem je nízké zaměření na danou látku ve školách. Většinou se zmínky o šifrách objevují jen v dějepisných předmětech a to jen jako informace o jejich zásluhách v historii, nikoliv však jejich implementace a další podrobnosti.

Cílem této práce je seznámit čtenáře se základy kryptologie, její historií, strukturou a popsat nejznámější šifrovací algoritmy. Ukázat jejich rozdíly a podobnosti v implementaci a postupu při šifrování.

Práce je rozdělena na teoretickou a praktickou část. Praktická část je program napsaný v jazyce C#, kde jsou vybrané šifry implementovány a lze je vyzkoušet, popřípadě porovnat odlišnosti jednotlivých zašifrovaných zpráv. Teoretická část se zaměřuje na popis kryptologie a jejich podoborů, což jsou kryptografie, neboli šifrování, kryptoanalýza, věda zabývající se prolomení šifer bez přístupu ke klíči k dešifrování a steganografie, obor ukrývání zpráv před přečtením.

2 Kryptologie

Kryptologie je věda skládající se z šifrování a dešifrování (kryptografie), luštění šifry (kryptoanalýza) a ukrývání komunikace (steganografie). Základem jejího názvu, stejně jako kryptografie a kryptoanalýzy, je řecké slovo kryptos (skrytý).

Všechny podobory dohromady se starají o celou práci okolo šifrování. O výběru vhodného typu zabezpečení a jejího použití se stará kryptografie. Ta má taky za úkol zašifrovaný text rozluštit. Kryptoanalýza je obor starající se o proniknutí k informacím bez důležitých vstupních parametrů, jako je třeba vstupní klíč. Steganografie řeší ukrývání celé komunikace před zpozorováním.

Informace k sepsání této kapitoly jsem čerpal z knih Kryptografie od Freda Pipera [1] a The Codebreakers od Davida Kahna [3].

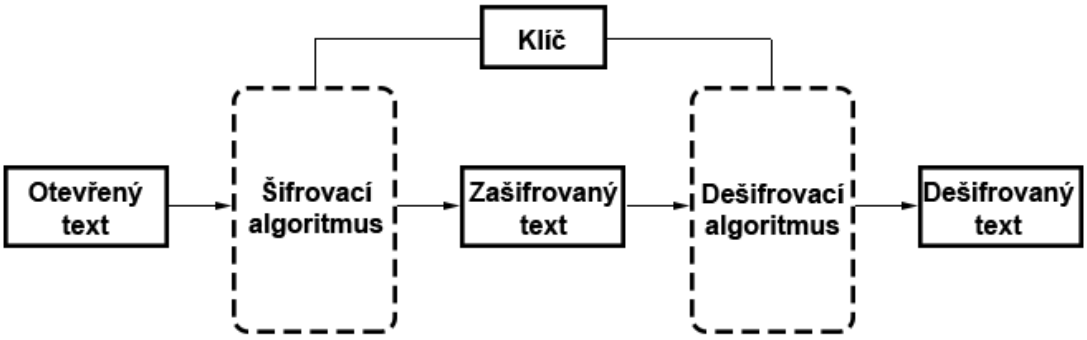
2.1 Kryptografie

Kryptografie má za úkol skrýt význam přenášeného textu převodem nezašifrovaného textu (*otevřený text*) do podoby, kdy si jej nikdo bez znalostí tajného kódu a algoritmu pro rozluštění nemůže přečíst. Nezaručuje to sice, že se výsledný text nedostane do cizích rukou, ale zajistí to, že bude pro tuto osobu nesrozumitelný. Výsledný text (*zašifrovaný text* nebo také *kryptogram*) však musí být možné převést zpátky do původní podoby na otevřený text. Proces zabezpečení zprávy z otevřeného textu na zašifrovaný se nazývá *šifrování* (viz obr. 1). Opačný proces, získávání otevřeného textu z textu zašifrovaného, se jmenuje *dešifrování*. Postup při převodu otevřeného textu do výsledného se nazývá *šifrovací algoritmus* a ten je závislý na zvoleném *šifrovacím klíči*, bez kterého není možné jednoduchou cestou získat původní text zprávy. Tento klíč je důležitý pro bezpečnost šifry. Musí mít dostatečnou délku a složitost. Pokud bychom využívali pouze jednoduchých klíčů, bylo by jednoduché prolomit šifru i základními metodami kryptoanalýzy, jako jsou třeba útok hrubou silou (postupné zkoušení všech možných klíčů) nebo slovníkový útok (použití vybraných klíčů). Najít bezpečný klíč je čím dál složitější. Zatímco v starších dobách nebyly prostředky na zjištění klíče, dnes se musí používat daleko složitější metody generování. Využívají se náhodné fyzikální jevy, hardwarový šum nebo nějaké pseudonáhodné generátory.

Obor kryptografie se v průběhu dějin vyvíjel a dnes jej můžeme rozdělit na dvě hlavní části. Jednou je klasická a druhou moderní kryptografie.

2.1.1 Klasická

Klasická kryptografie se vyznačuje svými malými požadavky na pomůcky k šifrování a dešifrování. Ve většině případů nám stačí jen tužka a papír popřípadě nějaké jednoduché nástroje. Taky můžeme říct, že v klasických šifrách se výhradně zaměřujeme na šifrování textu. Texty zašifrované šifrou řadící se do klasické kryptografie většinou zanechávají statistické informace o vstupním textu a tím jsou velmi snadno prolomitelné algoritmy kryptoanalýzy, jako je třeba frekvenční analýza. Pro svou jednoduchost jsou



Obrázek 1: Schématické znázornění šifrování

klasické šifry v dnešní době používány spíše jako pomůcky k hrám nebo jiným zábavným činnostem.

Klasickou kryptografii dále dělíme podle toho, jakým způsobem pracují s množinou písmen při šifrování. Prvním druhem šifer jsou substituční šifry a druhým jsou transpoziční šifry.

Substituční Šiframi substitučními označujeme šifry, které jako způsob přeměny textu z otevřených na zašifrované používají nahrazení (záměnu, substituci) podle určitého pravidla. Podle typu šifry pak nahrazený text může být písmeno, skupina písmen nebo také speciální znak. Znakům použitým pro zašifrovaný text říkáme nomenklátory. Dešifrování u substitučních šifer poté probíhá pomocí obrácené substituce.

Existuje několik různých druhů substitučních šifer. Dělíme je podle toho, s jakým množstvím znaků pracují a podle počtu substitucí na šifrovaný text. Pokud šifra pracuje s každým znakem samostatně je nazývána *jednoduchá substituční šifra*. Tento druh šifry je málo odolný proti frekvenční analýze. Pracuje-li se skupinou znaků, například s dvojicemi (bigramy) jde o *šifru polygrafickou*. U polygrafických šifer je výhoda že můžeme stejný znak šifrovat v jiných skupinách různě, což nám pomáhá v bezpečnosti. Dalším typem jsou *monoalfabetické* a *polyalfabetické* šifry. Monoalfabetické šifry se vyznačují tím, že používají jednu substituci pro celý text, což je velice jednoduché ale také málo bezpečné. I málo zkušená osoba dokáže tyto šifry jednoduše prolomit pomocí frekvenční analýzy. Oproti monoalfabetickým šifrám polyalfabetické využívají více různých substitucí v jednom textu. Tím jsou mnohem bezpečnější ale také složitější. Posledním druhem jsou *homofonní šifry*. Jedná se o vylepšené monoalfabetické šifry. Rozdíl spočívá v tom, že homofonní šifra umožňuje šifrovat jeden znak několika různými způsoby. Tyto šifry se používaly velice často kvůli své jednoduchosti a dostatečné bezpečnosti. V této době jsou už však zastaralé.

V dnešní době se substituční šifry pořád používají, ale jsou mnohem komplexnější a kombinují se s jinými technikami šifrování. Příkladem mohou být bitové blokové šifry DES a AES.

Transpoziční Na rozdíl od substitučních šifer, kde všechny znaky zůstanou na svém místě, jen jsou určitým způsobem přeměněny, fungují transpoziční šifry na způsob změny pořadí znaků ve zprávě. V zašifrovaném textu se tudíž objeví všechny znaky původního textu jen na jiném místě. Změna pořadí však musí být provedena podle nějakého pravidla, aby bylo možné zpětně získat původní text. Výhoda tohoto typu šifer je jejich velká jednoduchost. Protože není nutná znalost těžké matematiky, mohou je používat i děti. Nevýhoda je však velmi nízká bezpečnost.

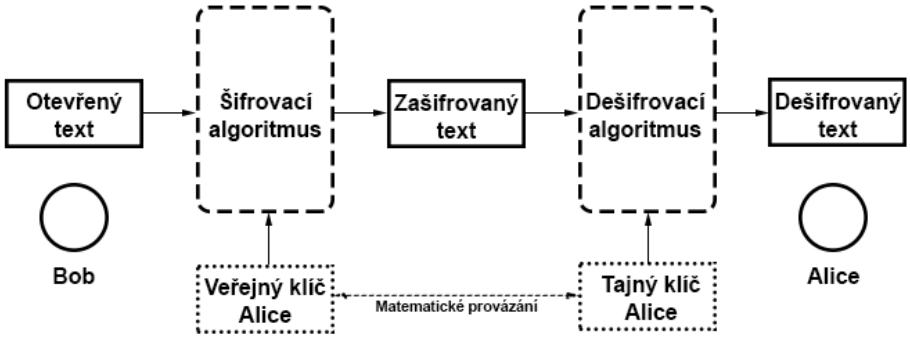
Transpoziční šifry nemají vymezené dělení jako u šifer substitučních. U většiny šifer se jako pomůcky používají různé geometrické tvary jako třeba koleje, sloupce, mřížky a podobné. Jako příklad můžeme uvést šifru *Rail Fence* u které se otevřený text sestupně píše na "koleje"jdoucí vedle sebe a když narazí na poslední, pokračuje se směrem zpět nahoru. Výsledná zpráva vznikne sepsáním písmen po řádcích. Dalším příkladem je *Route šifra*. V ní se nejdříve otevřený text zapíše do mřížky daných rozměru a potom se čte podle určeného klíče. Klíčem je vždy vzor kterým se prochází všechny pole mřížky. Jako klíč můžeme třeba zvolit levotočivou spirálu jdoucí z levého spodního rohu. Mezi transpoziční šifry dále patří šifry využívající slovo jako klíč. Dané slovo si převedeme na čísla podle abecedního pořadí jednotlivých písmen v klíči. Otevřený text si napíšeme do řádku o délce rovné počtu písmen klíče. Následná šifra vzejde sepsáním písmen z tabulky podle pořadí dané čísly klíče. Na tomto principu pracuje *Sloupcová transpozice*, *Dvojitá transpozice* a *Myszkowskiho transpozice*.

2.1.2 Moderní

S rozvojem techniky se staly klasické metody kryptografie zastaralé a příliš jednoduché na prolomení. Bylo nutné vymyslet komplexnější metody a algoritmy. Začaly se používat mechanické stroje, které zautomatizovaly a zrychlily elementární procesy a tím umožnily provádět náročnější úlohy v kratším čase. Po nástupu počítačů a po přesunutí většiny informací do digitální podoby se i kryptografie musela přizpůsobit. Šifrovací algoritmy začaly ve velké míře využívat matematické operace. Ty nepotřebují žádné specializované stroje, a tudíž se práce s nimi přesunula na počítače, kde využívají digitální podobu informací. To taky zapříčinilo, že se pracuje místo s jednotlivými znaky zprávy s jejich bitovým vyjádřením.

I v moderní kryptologii využíváme základní dělení. Jedna skupina je kryptografie *symetrická*. Řadí se do ní šifry využívající stejný klíč pro šifrování i pro dešifrování. Další skupinou je *asymetrická* kryptografie. Asymetrické šifry využívají dva odlišné klíče.

Symetrická Symetrické šifry využívají pouze jeden klíč. Jak pro šifrování, tak i pro dešifrování. Oproti asymetrickým šifrám jsou jednodušší a taky často mnohokrát rychlejší. Dá se proto jednoduše použít pro šifrování velkých objemu dat. Nevýhodou je nutnost bezpečně předat klíč mezi komunikujícími stranami. Kdokoliv totiž zjistí tajný klíč, může odposlouchávat celou budoucí komunikaci. Někdy se pro větší bezpečnost používají klíče vygenerované pro kratší časové úseky. Jedná se o takzvané klíče sezení (session key). Po prolomení jednoho klíče lze odposlouchávat komunikaci pouze do doby, než se vygeneruje nový klíč.



Obrázek 2: Schéma šifrování s veřejným a soukromým klíčem

U tohoto druhu šifer máme zavedené další dělení. Jsou to šifry *proudové* a *blokové*. Hlavní rozdíl je v práci s daty. Zatímco proudové pracují s jednotlivými znaky (typicky bity), blokové zpracovávají bloky bitů o stejné délce. Většinou bývá velikost bloku 64 bitů.

Mezi nejznámější symetrické šifry můžeme zařadit blokovou šifru DES, které je ale pro použití 56 bitů pro šifrování dnes překonatelná a tudíž považována za nedostatečnou. Jako náhrada je dnes používána šifra AES, která je stále nepřekonatelná.

Asymetrická Kryptografie s veřejným klíčem, jak je taky nazývána asymetrická kryptografie, na rozdíl od symetrické kryptografie využívá dva odlišné klíče. Jeden slouží pro zašifrování zprávy a druhý pro její dešifrování. Nejvíce využívaná verze tohoto typu kryptografie je použití takzvaného *veřejného* a *soukromého* klíče (viz obr. 2). Osoba, které chceme odeslat šifrovaná data, uvolní svůj šifrovací klíč veřejně. Kdokoliv jej může použít na zašifrování dat. Po přijetí zašifrovaných dat poté příjemce použije svůj soukromý klíč na dešifrování. Je nezbytné, aby oba klíče byly matematicky propojené, ale taky aby nebylo možné z šifrovacího klíče spočítat klíč dešifrovací.

Nevýhodou je pomalost šifrování i dešifrování, náročnost na prostředky a zdroje, a tím neefektivní šifrování velkého objemu dat. Často se proto používá spojení více šifer při komunikaci. Symetrickou šifrou se zašifrují požadované data a klíč k této šifře se zašifruj asymetrickou šifrou. Tím zajistíme bezpečnost a zároveň rychlost komunikace.

Příkladem dnes používaných asymetrických šifer je například šifra RSA nebo elektronický podpis.

2.2 Kryptoanalýza

Kryptoanalýza je proces získání původní zprávy z šifrovaného textu, kdy není k dispozici příslušný dešifrovací klíč. Jde o snahu najít slabinu v šifrovacím algoritmu a tu použít k zjištění otevřeného textu. Kryptoanalytikové využívají vědy, jako jsou matematika, lingvistika a fyzika.

K prolomení šifry se také používá metoda *útok postranními kanálem*. Jde o pokus využít informace zjištěné přímo z implementace celého kryptografického systému při běhu kryptografického algoritmu. Velmi často se tato metoda soustředí na zjištění dešifrovacího klíče. Pokud je zjištěná informace závislá na klíči šifrovacího algoritmu může útočníkovi pomoct klíč odhalit. Po úspěšném zjištění má útočník dostatečný počet informací které mu dovolí číst všechnu další komunikaci až do změny klíče. Ale cílem této metody není jen vypátrání klíče, ale třeba odhalení použitého kryptografického algoritmu, zjištění času běhu algoritmu a podobné, často velmi důležité údaje.

Kryptoanalýze se vyvíjí stejně jako kryptografie. I přes to že cíl je pořád stejný, dosažení cíle se měnilo podle toho, jaké šifry se v dané době vyvíjely. Celou kryptoanalýzu bychom mohli rozdělit stejně jako kryptografii a její vývoj. Klasická zahrnuje všechny metody, které se dají řešit papírem a tužkou, moderní které používaly komplexní stroje, jako byl třeba Britský stroj Bombe, použitý pro dešifrování slavné šifry Enigma, až po dnešní metody které jsou řešeny čistě matematikou. Nejznámější příklad moderních problému je rozklad prvočísel, který je pro dnešní úroveň techniky nesmírně náročný.

2.3 Steganografie

Pokud chceme skrýt obsah komunikace a komunikaci jako takovou, slouží nám k tomu obor steganografie. Tento obor má za úkol nejen zajistit, aby se nepovolaná osoba nedozvěděla o obsahu zprávy, ale také aby byla skrytá celá komunikace. Jedná se o takzvanou bezpečnost skrze utajení (security through obscurity). To znamená, že zachycení zprávy znamená taky její prolomení. Díky tomuto se často kombinuje s jinými metodami zabezpečení, hlavně šifrováním. Samostatná steganografie není v dnešní době považována za bezpečnou.

Do oblasti patří metody typu neviditelný inkoust a mikrotečky. V moderní době se do popředí dostává zejména digitální podoba steganografie. Do různých počítačových souborů lze vložit skrytý obsah, který nelze jednoduše odhalit. Nejideálnější typy souborů jsou bitmapy a zvukové soubory protože mohou obsahovat takzvaný šum, který se využívá pro přenos tajné informace a neznehodnocuje původní data.

3 Historie

Všechny informace v této kapitole jsem čerpal z knihy Kryptografie od Freda Pipera [1] a Knihy kódů a šifer spisovatele Simona Singha [2].

3.1 První kryptografie

První znaky ukrývání informací byly vypátrány už do doby kdy mnoho lidí ani neumělo číst a psát. Za nejstarší nález jsou považovány nestandardní hieroglyfy v památkách starověkého Egypta. Vědci je datují do období okolo roku 1900 před naším letopočtem. Další významné nálezy (1500 př. n. l.) jsou třeba jílové tabulky z Mezopotámie, které byly očividně napsány tak, aby ukrývaly význam jejího textu. Jednalo se o recepty hrnčíře, takže už tehdy používali kryptografii pro uchránění duševního vlastnictví nějaké osoby. V té době kryptografie nebyl moc známá ani rozšířená nauka. Větší zájem se dá vystopovat kolem roku 550 př. n. l. Jedná se o nejstarší známou šifru Atbash kterou využívali hebrejští učenci.

Velkému rozvoji šifer se dařilo v Antických dobách. Jako jedna z prvních zmínek o šifrování pocházejí od Herodota. Ve své knize Dějiny popisoval válku mezi Řeky a Peršany a označil umění posílat utajené správy jako hlavní důvod záchrany Řecka. Včasná zpráva, která nebyla rozluštěna nepřítelem, dovolila připravit se na nadcházející konflikt. Ve vojenské oblasti se využívala šifra Skytalé používána Spartánskou armádou (viz obr. 3). S nadsázkou jej můžeme označit jako první vojenský šifrovací přístroj. Jednalo se o tyč určitého průřezu a svitek kůže s písmeny. Po navinutí svitku na tyč se dala číst zpráva od jednoho konce tyče k druhému. Pokud svitek nebyl navinut, písmena spolu nedávaly smysl. Další známá byla pak třeba Caesarova šifra, která ve své době byla považována za velmi bezpečnou. Často byly využívány i metody steganografie kdy se například používalo tetování na hlavě otroka, které časem zarostlo vlasy anebo zpráva napsaná pod voskem.

Řekové jako velmi vzdělaný národ samozřejmě také přispěli k rozvoji kryptografie. Můžeme jim přiřadit Polybiův čtverec a také válečné knihy ve kterých se rozebírá několik typů šifrování.

Hodné známá je také zmínka o šifrách v knize Kámasútra. Kniha, mimo jiné, doporučovala ženám naučit se mnoho umění a mezi nimi na 45. místě bylo umění tajného psaní. Byla zde poprvé popsána šifra substituční. Doposud se využívaly hlavně šifry substituční.

3.2 Středověká kryptografie

Ve středověkých dobách můžeme za největší průkopníky označit Arabský národ. Kryptografie byla u nich vcelku rozšířená a používaná věda. Používali je jak normální lidé tak dokonce státní úředníci. Navíc Arabové jako první začali zkoumat šifry z matematického hlediska a zaobírali se také technikou jak šifry prolomit. Lidé do té doby neměli dostatečné znalosti matematiky, statistiky a také lingvistiky. Hlavní postavou byl Al-Kindi

Obrázek 3: Šifra Skytale - obrázek převzat z *wikipedia.org* [9]

který jako první popsal nejstarší techniku kryptoanalýzy a to je frekvenční analýza. Popsal také statistku rozložení písmen a kombinaci písmen v arabském jazyce. To byl největší posun v kryptoanalýze skoro až do 2. světové války. Tato metoda kryptoanalýzy byla účinná proti šifrám až do příhodu polyalfabetických šifer. Jako dalšího průkopníka můžeme zmínit učence Ahmeda al-Qalqashandiho. Je to autor 14 dílného spisu *Subh al-a 'sha* kde věnoval kapitolu kryptografii.

Oproti pokroku Arabů byla Evropa v oblastech kryptografie daleko pozadu. Zatímco Arabové objevovali metody luštění tak se Evropané potýkali pouze se základy šifrování. Mohla za to doba temna, která postihla Evropu. Lidé byli spíše přikloněni náboženství než vzdělanosti. Nejvíce práce s tajnými písmy bylo v té době v klášterech. Tamní mniši se snažili odhalit utajené významy, které se skrývají v bibli. Starý zákon prokazatelně obsahuje šifrované texty. Použití šifer ale nejspíše neměly za úkol ukrýt význam ale spíše navodit tajemnost. To stačilo na to, aby se rozvinul zájem o kryptografii. První evropská kniha o kryptografii byla napsána anglickým františkánem Rogerem Baconem. Kniha se jmenovala *De secretis artis et naturae operibus etde nullitate magae* (List o tajných dovednostech a neexistenci magie) a obsahuje informace jak sedmi metodami uchovat tajemství informací. Z literatury známý Geoffrey Chaucer také využíval šifry ve svých dílech. Namísto písmen ale používal symboly. Na první pohled bylo šifra bezpečnější, ale oproti tradičním šifrám s výměny písmen se složitost dešifrování neměnila.

Kolem 15. století už byla kryptografie velmi rozšířeným oborem. Nejvíce tomu pomohlo období renesance, kde se kladlo daleko větší důraz na vzdělanost než v dobách předchozích. Lidé se přestali obracet k bohu a věnovali svou pozornost vědě a učenosti. Rozvíjela se politika a tím i rostla potřeba tajit komunikaci. Centrem vývoje kryptografie byla Itálie. Jakožto stát, kde se renesance nejvíce rozvíjela, tak i seskupení mnoha městských států které bojovaly o nadvládu nad ostatními. Politika a diplomacie hrály významnou roli. Každá stát měl vlastní skupinu lidí věnující se šifrování a dešifrování. S tím se začala i v Evropě vyvíjet kryptoanalýza. Jako první velký evropský kryptoana-

lytik bývá označovaný Giovanni Soro. Od roku 1506 pracoval pro Benátskou republiku jako tajemník pro šifry. Byl svými schopnostmi tolik známý, že i spřátelené státy si od něj nechaly luštit zachycené šifry. Dokonce tehdejší papež Klement II. využíval jeho služby.

Dalším státem velmi se věnujícím kryptoanalýze byla Francie. Král František I. zaměstnával Philiberta Babou. Ten získal reputaci tím, že na prolomení šifry neúnavně pracoval třeba celé dny i noci. Jejich nejvýznamnější kryptoanalytik té doby však byl Francois Viete. Ten se zasloužil hlavně o dešifrování španělských šifer. Ti byli na svou dobu pozadu se znalostmi v kryptografii i kryptoanalýze a obrátili se dokonce na Vatikán s žalobou o spřažení s ďáblem.

Tato doba také poukázala na to jak je kryptografie pozadu oproti kryptoanalýze. Doposud se používaly pouze monoalfabetické šifry které byly prolomitelné frekvenční analýzou. Ti, kteří si to uvědomovali, se snažili vylepšit nebo pozměnit šifru tak aby jejich vzkazy nebyly tak jednoduché k prolomení. Někteří používali takzvané klamače, symboly nebo písma, jenž nepatří do zašifrovaného slova, ale slouží pouze k oklamání kryptoanalytika, nebo se také účelně psalo nespisovným jazykem, což změní statistické rozložení písmen a ztížilo prolomení. Dále se používalo kódování slov. Naproti substitučním šifrám kde se každé písmeno měnilo v jiné, u kódování se nahrazuje celé slovo jiným slovem nebo symbolem.

Větší změnu v kryptografii přinesl až florentský polyhistor Leon Battista Alberti narozen roku 1404. I když nevymyslel konkrétní šifru, vymyslel způsob jak vyřešit problém monoalfabetických šifer. Použít více šifrovaných abeced pro jeden text. Základ polyalfabetických šifer byl vymyšlen ale dále nerozvíjen. Až později, na konci 16. století, německý opat Johannes Trithemius, italský umělec Giovanni Porta ale hlavně francouzský diplomat Blaise de Vigener rozvedli Battistovy myšlenky. Zprvu se Vigener věnoval kryptografii pouze z pracovních důvodů, ale po skončení jeho kariéry se věnoval dalšímu studii kryptografie. Navázal na práce svých předchůdců a vymyslel Vigenerovu šifru. Výhodou této šifry je že nepoužívá pouze jednu šifrovací abecedu, ale až 26 abeced a to ji dává odolnost proti frekvenční analýze. Taky zde hraje poprvé velkou úlohu klíč šifry, kterým vybíráme pořadí šifrovacích abeced.

I přes své nesporné výhody se polyalfabetické šifry neujaly. Obyčejní lidé nepotřebovali své zprávy ochránit tak složitou šifru a v důležitějších odvětvích jako byla politika a vojsko odmítali použít tyto šifry pro svou náročnost. Nejvíce ve vojenské oblasti, kde byla důležitá rychlost a jednoduchost. Proto bylo nutné najít kompromis mezi bezpečností a rychlostí. Do popředí se dostalo použití homofonních šifer. I ony však svou povahou dávají možnost je prolomit a po krátké době byly zase nedostačující.

3.3 Kryptografie od 18. století do začátku první světové války

Na začátku 18. století začaly vznikat v mnoha státech kryptografické kanceláře, takzvané černé komnaty, které se věnovaly šifrování na nejvyšší úrovni. Nejlepší kryptografové dokázali rozluštit i ty šifry, které se považovaly za dostatečně bezpečné. Nejznámější kancelář byla *Geheime Kabinets-Kanzlei* ve Vídni. Procházely jí všechny dopisy a listiny z tamní pošty. Proto tamní kryptologové pracovali s jasným rozvrhem, aby měli čas prozkoumat dopis a poté jej znovu zapečetit a vrátit. S rozšířením černých komnat se ko-

munikace monoalfabetickými šiframi stala naprosto nedostačující a začaly se prosazovat polyalfabetické šifry.

Velice zajímavou postavou kryptografie 19. století je nesporně Brit Charles Babbage. Je známy za návrh konceptu, který byl předchůdcem moderního počítače. Ten navrhl poté, co si všiml nespočet chyb v matematických tabulkách počítaných lidmi, ale jako mnoho jeho projektů skončil nedokončeně. Během druhé světové války se však elektronická podoba tohoto stroje stala nástrojem velkého pokroku v kryptoanalýze 2. světové války. V našem tématu je ale znám za prolomení do té doby naprosto bezpečné Vigenerovy šifry. Bylo to na popud člověka, který tvrdil, že vynalezl nový druh šifry, která však byla pouze variací Vigenerovy šifry. Tento člověk tvrdil, že jeho šifra není prolomitelná, ale okolo roku 1854 jej Babagge prolomil. Využil přitom periodického použití klíče v šifře. Tento objev byl zaznamenán až v 20 století. Babbage, známý svým nedokončováním projektů jako je třeba velká kniha o šifrách, svůj objev nepublikoval. Až nezávisle na něm, roku 1863, byl zveřejněn Kasiského test bývalým důstojníkem pruské armády Friedrichem Kasiskim. Ten odpovídá Babbageho postupu. Jeden z důvodů nepublikování může být taky to, že britská rozvědka chtěla mít převahu nad svými protivníky a nechtěla dát vědět, že lze Vigenerovu šifru prolomit.

Kvůli těmto objevům se kryptografie v profesionální sféře dostala do špatného postavení. Kryptoanalytici měli vždy navrch nad kryptology. Ač se lidé snažili vymyslet nové druhy šifer, nenašla se žádná, která by byla natolik bezpečná, aby se dala použít v důležitých oborech. Naproti tomu byla v rozkvětu amatérská kryptografie. S rozmachem komunikace, zejména telegrafu, si lidé začali bránit své informace. Díky následnému velkému zájmu široké veřejnosti se kryptografie rychle začala rozšiřovat v literatuře 19. století. Můžeme zmínit tituly, jako jsou třeba Cesta do středu Země od Julese Verna, Návrat Sherlocka Holmese od Arthura Conana Doylea nebo mezi kryptology slavnou povídku Zlatý brouk kterou napsal americký spisovatel Allan Edgear Poe.

3.4 Kryptografie za první a druhé světové války

Technický rozvoj Po malém vývoji kryptologie na konci 19. století nastal velký převrat. Byl způsoben dvěma událostmi. Jednou byl vynález italského fyzika Guglielma Marconiho na přelomu 19. a 20. století. Byla jim podobná forma komunikace, jako byl telegraf, ale bez potřeby spojení elektrickým vedením komunikujících stanic. Spojení bylo realizováno přes rádiové vlny. Tím bylo umožněno spojení dvou izolovaných stanovišť. Nejdříve bylo velkým omezením krátká vzdálenost, po které se dalo komunikovat, ale tento nedostatek byl časem vyřešen a dalo se spojit i přes Atlantský oceán. Vynález byl okamžitě středem zájmů armády. Přes své výhody měl ale také jednu zásadní nevýhodu vyplývající z techniky všesměrového vysílání rádiových vln. Cokoliv bylo posláno, bylo možné přijmout kýmkoliv, třeba i nepřítelem. To kladlo velké požadavky na kvalitní zašifrování zpráv. Druhou událostí způsobující rozkvět kryptologie bylo vypuknutí 1. světové války. Všechny strany se snažily najít nějakou šifru, která by byla bezpečná na delší dobu. Bohužel se nikomu nedařilo. Kryptoanalýza byla vždy napřed a prolomení šifer bylo jen otázkou času. Jako příklad můžeme uvést německou šifru ADFGVX která spojovala substituci i transpozici.

Francouzská armáda byla v té době nejvíce vyspělá v kryptoanalýze. Vycházeli z práce Augusta Kerckhoffa *La cryptographie militaire* (Vojenská kryptografie). Naproti tomu Německo zřídilo odbor kryptografie až roku 1916. Dalším velkým pomocníkem spojenců v dešifrování byli Britové a Američané. Známým pojmem je britská Kancelář č. 40. Právě tam rozluštili šifru, takzvaný Zimmermannův telegram, o rozkazu neomezené ponorkové války Německa. A tímto objevem získali na svou stranu dosud neutrální Američany. Mnoha lidmi je tento moment považován jako zvrat ve válce.

První světová války byla význačná tím, že kryptologie byla pozadu oproti kryptoanalýze. Každá nasazená šifra byla za čas prolomena. Ke konci války však přišel americký vynálezce Gilber Vernam a příslušník armády Joseph Mauborgne s novým druhem šifry. Jednalo se o upravenou Vigenerovu šifru kde se délka klíče rovná délce vstupního textu. Pro zajištění co největší bezpečnosti navíc musí být klíč naprosto náhody a nesmí se nikdy opakovat. Tím zajistíme nemožnost útoku hrubou silou a taky že po zjištění části klíče nemůžeme nijak odvodit zbytek. Podle toho se šifra jmenuje jednorázová tabulková šifra (anglicky one time pad) nebo také Vernamova šifra. Tato šifra byla později, jako jediná, vědecky prokázána za naprosto neprolomitelnou při použití zcela náhodného klíče.

Následné problémy tohoto konceptu tak nebyly s bezpečností šifry, ale s generováním a distribucí klíče. Nejdříve se používaly knihy, které na všech stranách obsahovaly náhodné písmena. Muselo se však zajistit, aby obě stany komunikace měly naprosto stejné knihy. Používal se vždy první list a následně musel být zničen, aby se klíč neopakoval. Protože se ale komunikovalo velice často, byl problém s generováním a distribucí klíče. Vytvářet náhodné posloupnosti písmen není jen tak lehké. Nejbezpečnější je využít fyzikálních jevů jako je třeba radiace. Po vytvoření knihy s kódy je třeba je rozeslat mezi všechny účastníky komunikace. To je velice složité a často nebezpečné. Pokud by kniha padla do rukou nepřátel, je celá komunikace v ohrožení.

Tyto komplikace zapříčinily, že se šifra nezačala používat ve větším měřítku. Využívá se jen tam, kde je bezpečnost na prvním místě a nevadí komplikované procesy vytváření a distribuce klíče. Můžeme třeba uvést, že tato šifra zabezpečuje komunikaci mezi prezidenty Ruska a USA.

Kryptologové se však nevzdávali. Bylo ale zapotřebí udělat technologický pokrok. Přestali spoléhat na tužku a papír a začalo se přecházet na mechanické a elektrické stroje. Už v 15. století Leon Alberti vynalezl jeden z prvních šifrovacích strojů. Byly jim dva kotouče připevněné na sobě každý s abecedou po okraji. Tyto kotouče se daly nezávisle posouvat a tím sloužily jako pomůcka při šifrování a dešifrování mono a polyalfabetických šifer. Pro svou jednoduchost byl tento vynález, třeba s mírnými úpravami, používán až do 20. století.

Zrození Enigmy Roku 1918 založil německý vynálezce Arthur Scherbius se svým společníkem Richardem Ritterem firmu Scherbius & Ritter. Tam mimo jiné vyvinuli, a nechal si patentovat Enigmu (viz obr. 4). Nejznámější šifrovací stroj světa. Enigma se skládá z více menších součástí. Konkrétně propojovací deska, 3 rotory, reflektor, klávesnice a signalizační žárovky. Samostatně nejsou moc bezpečné, ale jejich důmyslné spojení dohromady dávalo velice složitou šifru. Způsob jak pracuje, byl známý. Bezpečnost proti

prolomení dosáhla velkým počtem možných vstupních klíčů. Těch bylo až 10 000 000 000 000 000. Jako klíč sloužilo počáteční nastavení všech komponent Enigmy. Scherbius se snažil svůj přístroj prodat jak obchodní sféře tak vojenské. Pro každý měl lehce jiný druh Enigmy. Kvůli své vysoké ceně však nebyla kupována. Ani pozdější stát proslavený Enigmou, Německo, nechtělo utrácet. Nebyli si totiž vědomi prolomení svých šifer.

Až postupem času si Němci uvědomili, že jejich šifry nejsou bezpečné a že je musí nahradit. Po prozkoumání všech dostupných možností došli k závěru, že nejlepším řešením bude nasazení Enigmy. Velkovýroba začala roku 1925. V následujících 20 letech jí Scherbius prodal armádě na 30 tisíc kusů. Ty se lišily vnitřním nastavením od přístrojů prodaných do veřejného sektoru. Německo tak bylo na začátku 2. světové války nejlépe vybavená země v oboru kryptografie.

Krátce po nasazení Enigmy začali britští kryptoanalytici v Kanceláři č. 40 získávat jejich zašifrované zprávy. Nikdo však nemohl přijít na způsob jak je rozluštit. Ani jejich spolupracovníci Franci a Amerika nemohli dosáhnout žádného pokroku. Informací získaných z odposlechů bylo pořád méně. Po výhře v první světové válce nabyli spojenci neoprávněného pocitu bezpečí. Proto nevěnovali prolomení nového typu šifry velký důraz. Jediný stát, který byl pořád ve střehu, byl Polsko. Věděli, že mír nebude trvat dlouho a chtěli být připraveni předem na další postup Německa. Založili své vlastní šifrovací oddělení Biura Szyfrow. Ta vlastnila komerční verzi Enigmy, ale ta se lišila vnitřním nastavením rotorů. Zjištění nastavení bylo nutné k dalšímu postupu s dešifrováním. Překvapivě bylo toto nastavení získáno od Němce Hanse-Thilo Schmidta který nebyl spokojen s vývoje Německa po první světové válce a se svým postavením ve společnosti. Ten za příslib získání peněz, díky své práci v úřadu šifrovaných komunikací, získal důležité dokumenty o Enigmě a prodal jej francouzskému agentovi s krycím jménem Rex. Z těchto dokumentů bylo možno zjistit tolik potřebné zapojení rotorů.

Spojenci tedy měli možnosti postavit přesnou kopii vojenské Enigmy. Ale i s tím nebylo možné šifru prolomit. Největší bezpečnost stroje byla v obrovském množství možných klíčů. Francouzi, vlastníci dokumentů, kvůli tomu ani nezkoušeli Enigmu sestrojit. Protože však dříve podepsali s Polskem smlouvu o vojenské spolupráci a pro velký zájem Polska o Enigmu předali tyto dokumenty do kanceláře Biura Szyfrow. Ti ze strachu z Německé invaze, začali zjišťovat, jak by bylo možné klíč získat. Další ztížení bylo to, že Němci aby neulehčili protivníkům dešifrování tím, že denním klíčem zašifrují obrovské množství textu, z kterého se dají lépe vyčíst nedostatky, používali denní klíč k zašifrování klíče k následné komunikaci.

Poláci zjistili, že jazykovědci, kteří byli do té doby nejlepší v prolamování šifer, si nemůžou s novým typem šifry poradit. Protože to byla šifra mechanická, hledali na tuto práci matematiky. Uspořádali tajný konkurz pro získání dalších spolupracovníků. Tři nejlepší poté zaměstnali. Nejlepší z nich byl dvacet tři roků starý Marián Rejewski. Po nějakém čase stráveným prací v Biuro Szyfrow byl převelen na práci s Enigmou. Snažil se najít cestu přes pokyn Němců posílat nový klíč komunikace dvakrát za sebou z důvodů možné chyby. Za chvíli našel určitá propojení mezi skupinou písmen. Pokud dostal dostatečné množství zpráv, dokázal sestavit všechny vztahy. Všiml si, že každý den se vztahy mění. Znamenalo to, že jsou svázány s denním klíčem. Ještě však nebylo v jeho

silách z obrovského množství možných klíčů odvodit ten pravý. Snažil se tedy tuto množinu zmenšit.

Zjistil, že nastavení rotorů a propojovací desky Enigmy mají vliv na podobu zprávy, ale propojovací desky neměly vliv na délky vztahů, jež zjistil předtím. To mu dalo možnost řešit jednodušší problém než nalezení denního klíče. Jaká kombinace rotorů odpovídá zjištěným vztahům. Rotory byl v té době 3. To dávalo počet 105 456 možných kombinací, což je zhruba sto miliardkrát menší než počet klíčů. Musel si zaznamenat vztahy z každých možných kombinací. To jeho týmu trvalo celý rok. Poté bylo možné začít s dešifrováním. Každý den sestavil z příchozích zpráv nové vztahy. Ty porovnal s těmi zaznamenanými. Tím zjistil nastavení rotoru pro daný denní klíč. Poté jen zbývalo najít kombinaci propojovací desky. To zjistil postupným zkoušením a vylučováním možností.

Tímhle objevem najednou byla Německá komunikace zase jednoduše čitelná. Nebyla sice ještě válka ale její hrozba ano. Prolomení Enigmy je nesmírně náročný úkol a Rejewski jej zvládl. Po čase sestrojil mechanický stroj, který vyhledával aktuální nastavení. Pro 6 různých uspořádání rotorů bylo sestrojeno 6 těchto přístrojů, které pracovaly paralelně. Stroje se pro svůj charakteristický zvuk nazývaly *bomby* a dokázaly za zhruba 2 hodiny najít aktuální nastavení.

Německo ale na konci roku 1938 zvětšilo bezpečnost Enigmy tím, že přidali 2 nové rotory a zvýšili počet propojení propojovací desky z 6 na 10. Počet uspořádání rotorů se zvedlo z šesti na šedesát a místo dvanácti přehozených písmen bylo dvacet. Klíčů bylo najednou 159 000 000 000 000 000 000. Pro prolomení by bylo nutné zvýšit počet bomb desetkrát. To však bylo nad možnosti polského Biura. S rostoucí hrozbou ze strany Německa si Polsko uvědomilo, že nemůže doposud tajný objev prolomení Enigmy držet před spojenci v tajnosti. Těsně před začátkem války byli informováni Francouzi a Britové. Ti byli překvapeni pokrokem Polska. Byly jim poslány všechny doposud zjištěné informace a výzkumy aby v nich pokračovali.

Pád Enigmy Britové po vzoru Polska začali do svých kryptografických řad nabírat místo lingvistů spíše matematiky a vědce. Byli přijímáni kolegové pracovníků Kanceláře č. 40 a taky absolventi z univerzity v Cambridgi. Původní pracoviště v Londýně už bylo nedostačující. Přemístili se tedy o Bletchley Parku v Buckinghamshire kde sídlila takzvaná Government Code and Ciphet School. Ta postupně nahrazovala Kancelář č. 40. Kolem tamního sídla se začaly stavět nové budovy. V každé se specializovali na určitý úkol, jako bylo luštění komunikace německé armády, luštění námořní Enigmy, nebo třeba překlad informaci. Z původních 200 zaměstnanců se za pět let Bletchley Park rozrostl na 7000.

Koncem roku 1939 se díky informacím získaným od polské Biuro Szifrow a díky většímu počtu zaměstnanců a zdrojů dařilo vědcům z Bletchley Parku prolomit posílenou šifru Enigmy. Každý den po půlnoci začali se získáváním nového denního klíče. To trvali i pár hodin. Po jeho zjištění však měli možnost do konce dne číst německé zprávy. Někdy jim to umožňovali samotní němečtí operátoři. Aby se nemuseli namáhat vymýšlet náhodné klíče, zvolili třeba na klávesnici 3 po sobě jdoucí písmena. Jako první se tedy testovaly tyto kombinace.

Obrázek 4: Šifrovací stroj Enigma - obrázek převzat z *thehistoryblog.com* [10]

Další slabinou bylo, že lidé, kteří sestavovali knihu s kódy, se nelogicky rozhodli, že žádný rotor nesmí být na stejném místě dva dny po sobě. Ač tím chtěli dosáhnout větší různorodosti, pro kryptoanalytiky to bylo velké ulehčení. Po zjištění pořadí z jednoho dne mohli automaticky vyřadit určitá nastavení pro následující den. Tohle jim ulehčilo práci zhruba o polovinu. Podobné ulehčení jim přinesl pokyn, že nesmí být na propojovací desce propojeny sousedící písmena. To taky působilo kontraproduktivně pro bezpečnost šifry.

I přes tato ulehčení byla stále potřeba hledat nové cesty prolomení. Enigma se neustále vyvíjela a vylepšovala. Proto se musely vyvíjet i metody prolomení, stroje bomby a metody k získání každého detailu o šifře. Velkou pomocí byla velká sestava matematiků, lingvistů, přírodovědců a fyziků v každé budově. Po zjištění problému se jej někdo pokusil vyřešit. Pokud to nedokázal, předal tento úkol někomu jinému. Tak to pokračovalo, dokud někdo problém nevyřešil úplně. Pokud byl jen částečně vyřešen, pokračovalo předávání problému na dalšího. Přes nespočet lidí, kteří vykonali záslužné kryptoanalytické objevy, byl jeden, který se tyčil nade všemi. Jmenoval se Alan Turing.

Roku 1931 byl Turing přijat na King's College v Cambridgi. Tam také publikoval práci *On Computable Numbers* (O vyčíslitelnosti), která ho vědecky proslavila. V ní se píše o problému nerozhodnutelnosti. Použije tam pomyslný stroj, který podle potřeby provádí matematické operace na vstupních datech vložených na pásce a poté tiskl výsledek na výstupní pásku. Nejdříve měl být pro každou matematickou operaci jeden stroj. Později ale vmyslel stroj, který se řídí podle instrukcí. Jeden stroj tak zastane práci všech. Nazval jej univerzální Turingův stroj. Bohužel v té době ještě nebyly prostředky taková stoj vytvořit. V době tohoto vynálezu mu bylo 26 let.

Po pár letech práce jako učitel na cambridgeské byl pozván do Bletchley Parku aby se stal kryptoanalytikem. Nejdříve se podílel na běžné práci prolamování kódů. Poté se Turing soustředil na dalším postupu, kdyby Němci změnili způsob distribuce klíčů k Enigmě. Současná metoda vycházela z práce Rejewskiho kde se využívalo dvojí posílání klíče šifry. Britové si byli vědomi, že se Německo dovtípí, kde udělalo v současném systému chybu.

Na Turingovi bylo najít nový způsob prolomení, který by nezávisel na opakování klíče. Po nějakém čase přišel na to, že může využít rozsáhlou knihovnu s doposud rozšifrovanými zprávami. Důkladnou studií těchto materiálu zjistil, že velké množství z nich mělo danou pevnou strukturu, a že by se dalo předpovědět část textu nových zpráv porovnáním se starými zprávami.

Němci například každý den krátce po 6. hodiny posílali zprávy o počasí. Zpráva tudíž obsahuje slovo *wetter*, německý překlad slova počasí. Pomohl jim i vojenský styl zpráv, který byl velice striktně nastaven. Poté už nebylo složité odhadnout, které zašifrované slovo odpovídalo hledanému slovu. Takto propojeným dešifrovaným a šifrovaným slovům se říká tahák.

Turing věděl, že pokud bude mít tuto nápovědu, dokáže najít nastavení Enigmy, které je aktuálně použito. Teoreticky stačilo zkoušet jednotlivá nastavení Enigmy, dokud nenarazí na to správné. Ale to by z důvodů velkého množství klíčů bylo nemožné. Aby nebylo nutné zkoušet všechny možnosti klíče, snažil se Turing využít práci Mariána Rejewskiho.

Chtěl oddělit nastavení propojovací desky od nastavení rotorů. S použitím taháků našel podobné vztahy mezi skupinami písmen jako jeho Polský předchůdce. Po dalším výzkumu zjistil, že s použitím více strojů Enigma propojených mezi sebou dokáže jednoduše určit které nastavení je to pravé. S použitím dalších vynálezů a vylepšení nakonec přišel na to, jak mechanicky zjisti nastavení rotorů. Po zjištění nastavení rotorů stačilo jen vyřešit propojování na desce, což byla lehká úloha.

Bletchley Park získal dostatečné prostředky na realizaci Turingového výzkumu na fungující zařízení. Pro podobnost s Polským strojem na prolomení Enigmy jim říkali bomby. Každá bomba obsahovala dvanáct sad elektricky spojených rotorů. Po nějakém čase dorazily hotové zařízení a byly hned vyzkoušeny. Zklamání přišlo z rychlosti práce bomby. Nalezení klíče trvalo až týden. Turing s dalšími vědci začal pracovat na vylepšení stroje. Mezitím Němci změnili styl přenosu klíče. To způsobilo, že Britové nebyli schopni číst jejich depeše a nemohli získat žádné nové informace. Až po doručení nové bomby, která nebyla závislá na způsobu distribuci klíče, bylo možné zase získávat německé zprávy. Nové bomby stačily v lepších případech prolomit Enigmu již za hodinu.

Nebyla to slabost Enigmy, která tohle umožnila, ale nález taháku. Ty se staly hlavním prvkem k překonání šifry. U nich bylo nutné přiřadit zašifrované části textu tu správnou nezašifrovanou. K tomu pomohla vlastnost Enigmy, kdy nemohla zašifrovat žádné písmeno na sebe sama.

Další vítězství kryptoanalýzy Bohužel ale toto prolomení neznamenalo prozrazení celé německé komunikace. Třeba námořnictvo využívalo bezpečnější Enigmu, byli důkladnější v sestavování klíčů a jejím používání. Z toho důvodu byli vždy napřed před Spojeneckým námořnictvem a vyhrávali strategickou bitvu o Atlantský oceán. Vyřešením tohoto problému bylo ukradení knihy klíčů přímo od Němců. Muselo to však být uděláno tajně, aby nepřítel nepojal podezření a nezměnil způsob komunikace.

Kromě prolomení Enigmy byli kryptoanalytici u Bletchley Parku odpovědní za dešifrování zpráv Japonců a Italů. To pomohlo Spojencům hlavně v bitvách okolo Středního moře.

Informace ze všech zdrojů byly souhrnně nazývány Ultra. Podle mnoha lidí právě tyto informace zvrátily válku. To však nemůžeme v této době nijak dokázat. Nesporně však urychlili průběh války a zachránili nespočet lidských životů.

Po ukončení války byl Bletchley Park uzavřen. Schopnost číst nejtajnější šifry byla uchována jako národní tajemství. Vše co by mohlo prozradit tuto schopnost, bylo zničeno. Nové ústředí kryptografie bylo Government Communication Headquaters (GCHQ) v Londýně. Někteří pracovníci přešli na nové pracoviště a někteří se vrátili ke svým civilních životů zavázaní slibem mlčenlivosti. Až po 30 byla existence a výsledky Bletchley Parku uveřejněny.

Prolomení Enigmy a Purple bylo velkým vítězstvím kryptoanalýzy. Nebylo by to asi možné, pokud by byly používány správně. To znamená bez opakování klíčů, bez jednoduchých klíčů a bez opakování struktury zpráv, ze kterých bylo možné odvodit taháky.

Bezpečnost šifrovacích strojů bylo předvedeno přístroji Typex, který používala britská armáda a letectvo, a americkým vojenským přístrojem SIGABA. Tyto přístroje byly

konstrukčně složitější a tudíž bezpečnější než Enigma a navíc byly používány tak aby nedaly protivníkům nápovědy tak jako používání Enigmy. Tyto spojenecké přístroje byly nepřekonané po celou 2. světovou válku.

Tak jako Britové sklízeli úspěchy na poli kryptologie 2. světové války v Evropě, tak podobně se dařilo Američanům v bitvě o Pacifický oceán. Prolomení japonské strojové šifry Purple vedlo k odhalení mnoha plánů. Mezi nejznámější přípravy bitvy o Midway nebo cesta admirála Isoruka Yamamota.

Tajný jazyk Válka v Tichomořské oblasti také ukázala, že šifrovací stroje jsou sice velmi bezpečné, ale pro bojové podmínky velice pomalé. Pro komunikaci je potřeba celou zprávu po písmenech napsat na přístroji. Zašifrovanou zprávu poté předat radistovi, který jí pošle. Další radista jej příjme a musí jí předat kryptologovi. Ten po správném nastavení přístroje znovu vkládá zašifrovaný text a přepisuje na dešifrovaný. To bylo nepřípustné pro boje na malých tichomořských ostrůvcích, kde bylo zapotřebí reagovat co nejrychleji.

Vyřešení tohoto problému nabídl, byl inženýr Philip Johnson. Vymyslel kódový systém, který vycházel z řeči indiánského kmene Navaho, mezi kterými jako malý vyrůstal. Mimo tento kmen existovalo pouze pár lidí, kteří dokázali rozumět jejich jazyku. Po počátečních zkouškách byl nápad přijat. Dále bylo nutné vybrat jazyk, kterým se bude komunikovat. Nakonec byl vybrán jazyk kmene, u kterého tento nápad vznikl. Navahové byli jediný kmen, který nebyl dříve zkoumán Německými studenty, a tudíž bylo jasné, že jejich jazyk není prostudovaný. Navíc je Navažský dialekt, patřící do skupiny jazyků na-dene, naprosto odlišný od každého jiného. Tak bylo zajištěno, že nepůjde lehce prolomit.

Bylo vybráno 29 Navahů, kteří podstoupili kurz v komunikaci u námořnictva. Musel se však překonat problém, kde jejich jazyk neměl slova pro moderní válečné prostředky. Byl tedy vytvořen slovník, kde byly nepřeložitelná slova zakódované do slov, které jim přiřadili. Použité byly přírodní termíny. Například pro letadla to byly jména ptáků, pro lodě ryby a podobně. Taky byl problém se slovy, která se používají jen málo, nebo se jmény lidí a států. Proto se vymyslela fonetická abeceda, která se skládala ze jmen zvířat. Účastníci kurzu se museli naučit všechny tyto věci za 8 týdnů. Neexistovala žádná kniha, kde by tyto věci byly zapsány, a tudíž se nepřítel nemohl dozvědět jejich šifru. Po zkoušce kdy nahrávku poslali do kryptoanalytického oddělení, kde ani největší odborníci nemohli překonat tuto šifru, bylo jasné, že projekt je úspěšný.

V prvních dnech nasazení, koncem roku 1941, bohužel nastaly zmatky. Někteří radisté nebyli seznámeni s nasazení Navahů. Po odposlechnutí jejich depeší byli zmateni a hlásili, že nepřátelé komunikují na jejich frekvencích. Po čase se ale takové přehmaty odstranily a kód splňoval všechny předpoklady. Byl dokonale bezpečný a rychlý. Jediné slabé místo tohoto kódu bylo hláskování nepřeložitelných slov. Proto se do slovníku přidaly další slova. Pro zbytek hláskování se přidaly další zástupné slova, aby nebylo možné použít frekvenční analýzu. Navahové hráli významnou roli ve strategii Amerických sil. Celkově jich bylo 240. I přes jejich zásluhy, stejně jako o práci z Bletchely Parku, byla jejich práce státním tajemstvím. Až v roce 1968 byl kód Navaho odtajněn a mohlo se jim dostat ocenění. Navažský kód byl jeden z mála, který nebyl prolomen.

Další velký krok v kryptografii a vědě celkem přišel opět z Bletchley Parku. Kromě bomb, které dešifrovaly Enigmu, sestrojili Collosus. Ten byl zkonstruován k překonávání šifry Lorenz. Šifrovalo se přístrojem podobným Enigmě ale daleko složitějším. Byla však odhalena slabina v používání šifry a ta vedla k prolomení. To však vyžadovalo schopnosti, které bomba nebyla schopná z technických důvodů poskytnout. Proto museli kryptoanalytici ručně pracovat na proniknutí. To někdy trvalo až 2 týdny a prolomené zprávy již nebyly aktuální. S návrhem jak práci na Lorenzově šifře zautomatizovat přišel matematik Max Newman. Návrh jeho přístroje vycházel z konceptu univerzálního stroje Alana Turinga. Byl navržen tak aby se přizpůsobil různým problémům. Sestrojit takový stroj bylo na tu dobu velice těžký úkol. Kvůli tomu byl nejdříve tento projekt odložen.

To se nelíbilo inženýrovi Tommymu Flowersovi. Flowers strávil 10 měsíců na konstrukci tohoto přístroje. Konečný stroj byl 8. prosince 1943 dopraven do Bletchley Parku. Colossus byl sestaven z 1500 elektronek, které pracovaly daleko rychleji než relé použité v bombách. Zásadnější ale bylo to, že tento stroj byl programovatelný. Bohužel však všechna dokumentace musela být po skončení Bletchley Parku zničena. Až pozdější odtajnění mu přinesly zásluhy na sestrojení prvního předchůdce moderního počítače.

3.5 Moderní kryptografie

Počítačový věk Poválečné období v kryptologii bylo jednoznačně ovlivněno počítačem. Pro svou univerzálnost se na něm daly naprogramovat všechny známé šifry. Není omezen tak jako mechanické stroje. Dále je neporovnatelně rychlejší. Největší rozdíl je s prací s textem. Počítač pracuje s jejím binárním vyjádřením. Písmena můžeme vyjádřit jako posloupnost jedniček a nul. Používá se třeba ASCII standart (viz obr. 5). To však nemění nic na způsobu šifrování, kde se pořád využívá substituce nebo transpozice. Jakýkoliv kryptografický proces se skládá z těchto elementárních operací.

V počátcích počítačů bylo šifrování s nimi velice omezené. Počítače vlastnila pouze vláda a armáda. Až vynález tranzistoru roku 1947 inženýry z americké laboratoře AT&T umožnil jejich rozšíření. V dalších letech už byly počítače komerční záležitostí. Objevil se jeden z prvních programovacích jazyků, Fortran. Lidé měli možnost psát své vlastní programy. V roce 1959 byl vynalezen integrovaný obvod, což vedlo k zvětšení výkonu a snížení ceny počítačů.

Firmy začaly používat počítače ke komunikaci a ta musela být velice často šifrována. S rostoucím počtem počítačů bylo nutné, aby se věc zašifrovaná na jednom počítači dala dešifrovat na jiném. Proto se začalo jednat o standardizaci. Americký standardizační úřad zadal požadavek na šifrovací systém, který by mohl být používán firmami. Jeden z možných kandidátů byl systém firmy IBM nazývaný Lucifer. Ten i přes prvotní odpor amerického bezpečnostního úřadu NSA, který chtěl mít přehled nad všemi kryptografickými výzkumy a možnost prolomit každou šifru, byl nejlepším kandidátem.

Lucifer šifroval bloky po 128 bitech. Proces šifrování se měnil podle vstupního klíče, kterým bylo předem dohodnuté číslo. Byl velice rozšířený a bylo jasné, že se stane americkým standardem. Kvůli své bezpečnosti byl sledován NSA. Ta, aby měla možnost šifru prolomit, se zasadila, aby byl omezen počet vstupních klíčů. Klíč je zásadní v bezpečnosti šifry. NSA chtěla, aby se používal 56 bitový klíč. Ten je pro firmy dostatečné bezpečný,

ale NSA, která byla vybavena nejvýkonnější technikou, jej byla schopná prolomit. Lucifer byl tak na konci roku 1976 uznán jako americký šifrovací standard a byl nazván Data Encryption Standard (DES).

Problém distribuce Po vyřešení standardu byla kryptografie na počítačích využívána stále častěji. To však ukázalo na nový problém. Tím byla distribuce klíčů. Nejdříve se využívalo služeb kurýrů. Ti jezdili po celém světě a před komunikací museli doručit klíč od jedné komunikující strany k druhé. S rostoucím počtem komunikace byla tato metoda neúnosná.

Distribuce klíčů byla záležitost, která trápila kryptology už dlouho. Armáda a vláda se z počátku vypořádali tak že využívali svou moc a prostředky ale soukromý sektor byl velice omezená. Museli se spoléhat na třetí stranu, která tuto distribuci zařídila. To byl velmi velký bezpečnostní problém.

Až v polovině 70. let byl tento problém vyřešen. Zasloužili se o to kryptograf Whitfield Diffie, profesor Martin Hellman počítačový vědec Ralph Merkle. Diffie byl nezávislý inženýr v počítačové kryptografii a problém distribuce klíče ho velmi zajímal. Část jeho práce předpovídala globální propojení počítačů. Tato vize se v té době začala rozvíjet díky skupině ARPA a jeho propojení armádních počítačů ARPANet. Ten byl přímým předchůdcem internetu, který používáme dodnes. Už tehdy Diffie předpokládal, že aby lidé mohli bezpečně komunikovat je nutné šifrování jejich komunikace. To však potřebuje distribuci klíčů. Bohaté organizace a vláda toto mohla vyřešit svými prostředky, ale obyčejní lidé jsou v tomto velice omezeni. Tím mohlo být narušeno soukromí v moderním digitálním světě.

Po přednášení v laboratořích Thomase J. Watsona v roce 1974, kde tamější inženýři nesdíleli jeho optimistické představy, se dozvěděl, že před časem s podobnými myšlenkami přišel profesor Martin Hellman. Diffie se okamžitě vydal za Hellmanem. Tomu se moc setkání s neznámým Diffiem nelíbilo, ale nakonec přijal. Po schůzce byli oba nadšeni a za nějaký čas spolu začali pracovat na vyřešení problému distribuce klíče. Později se k nim přidal Ralph Merkle a snažili se najít alternativu k zdlouhavému a nákladnému fyzickému dopravování.

Pomocí k jejich hledání byla myšlenka, kdy spolu chtějí tajně komunikovat Alice a Bob. Alice vloží svou zprávu do skříňky a tu zamkne klíčem. Klíč pak musí dostat k Bobovi. Doposud bylo možné buď předat klíč osobně, nebo ho po někom poslat. Novým nápadem bylo, že Alice zamkne zprávu, pošle skříňku Bobovi, ten přidá svůj zámek a pošle skříňku zpět. Alice odstraní svůj zámek a znovu pošle skříňku Bobovi. Ten pak odstraní svůj vlastní zámek a může si zprávu přečíst. Tato metoda nevyžaduje výměnu klíčů, což odstraňuje velký problém moderního šifrování.

Objevuje se tu však další problém. U moderního šifrování je důležité pořadí šifrování a dešifrování. Pořadí musí být takové, že poslední šifrování se musí dešifrovat jako první. Výše zmíněný příklad toto pravidlo porušuje a to brání jeho přímé implementaci. I přes její omezení Diffie a Hellman vycházeli z této myšlenky.

Zaměřili se na matematické studium funkcí. Nejvíce se zajímali o funkce jednosměrné, což jsou takové, kde jde jednoduše zjistit jejich výsledek, ale zjistit vstupní parametry je

Ctrl	Dec	Hex	Char	Code
^@	0	00		NUL
^A	1	01		SOH
^B	2	02		STX
^C	3	03		ETX
^D	4	04		EOT
^E	5	05		ENQ
^F	6	06		ACK
^G	7	07		BEL
^H	8	08		BS
^I	9	09		HT
^J	10	0A		LF
^K	11	0B		VT
^L	12	0C		FF
^M	13	0D		CR
^N	14	0E		SO
^O	15	0F		SI
^P	16	10		DLE
^Q	17	11		DC1
^R	18	12		DC2
^S	19	13		DC3
^T	20	14		DC4
^U	21	15		NAK
^V	22	16		SYN
^W	23	17		ETB
^X	24	18		CAN
^Y	25	19		EM
^Z	26	1A		SUB
^[	27	1B		ESC
^\	28	1C		FS
^]	29	1D		GS
^^	30	1E	▲	RS
^-	31	1F	▼	US

Dec	Hex	Char
32	20	
33	21	!
34	22	"
35	23	#
36	24	$
37	25	%
38	26	&
39	27	'
40	28	(
41	29	)
42	2A	*
43	2B	+
44	2C	,
45	2D	-
46	2E	.
47	2F	/
48	30	0
49	31	1
50	32	2
51	33	3
52	34	4
53	35	5
54	36	6
55	37	7
56	38	8
57	39	9
58	3A	:
59	3B	;
60	3C	<
61	3D	=
62	3E	>
63	3F	?

Dec	Hex	Char
64	40	@
65	41	A
66	42	B
67	43	C
68	44	D
69	45	E
70	46	F
71	47	G
72	48	H
73	49	I
74	4A	J
75	4B	K
76	4C	L
77	4D	M
78	4E	N
79	4F	O
80	50	P
81	51	Q
82	52	R
83	53	S
84	54	T
85	55	U
86	56	V
87	57	W
88	58	X
89	59	Y
90	5A	Z
91	5B	[
92	5C	\
93	5D	]
94	5E	^
95	5F	_

Dec	Hex	Char
96	60	`
97	61	a
98	62	b
99	63	c
100	64	d
101	65	e
102	66	f
103	67	g
104	68	h
105	69	i
106	6A	j
107	6B	k
108	6C	l
109	6D	m
110	6E	n
111	6F	o
112	70	p
113	71	q
114	72	r
115	73	s
116	74	t
117	75	u
118	76	v
119	77	w
120	78	x
121	79	y
122	7A	z
123	7B	{
124	7C	|
125	7D	}
126	7E	~
127	7F	⌂

Obrázek 5: Část ASCII tabulky - obrázek převzat z *msdn.microsoft.com* [11]

nemožné. Nejvíce takových funkcí můžeme nalézt v modulární aritmetice. Ta pracuje s konečnou množinou čísel, které se určují podle funkce modulo. Po pár letech práce v modulární aritmetice, v roce 1976, přišel Hellman na nápad jak odstranit nutnost posílat klíč. Jeho nápad využíval jednosměrnou funkci:

$$a \equiv m^x \pmod{n} \tag{1}$$

Alice a Bob se veřejně dohodnou na číslech m a n. Tyto čísla mohou být klidně odposlechnuta. Poté si oba určí své tajné číslo x. Po vypočtení rovnice se svým číslem pošlou klíč zase veřejně svému protějšku. Zatím žádné z použitých čísel není klíčem, tudíž nevadí, pokud bude odposlechnuto. Číslo, které dostali, použijí ve stejné rovnici místo čísla m. Výsledek této rovnice vyjde oběma stranám stejně a je pak klíčem komunikace. Informace, které si Alice a Bob předali, jsou dostačující, aby se dohodli na klíči, ale třetí osobě nedovolují tento klíč zjistit.

Po odhalení tohoto objevu ihned kontaktoval své kolegy, kteří byli jedni z mála, kteří věřili, že se problém distribuce klíče vyřešit. Diffie, Hellman a Merkel svůj objev uveřejnili na National Computer Conference v roce 1976. Experti byli objevem ohromeni. Dokonce se musely přepisovat pravidla o kryptografii.

Tento systém výměny klíče odstranil jeden problém, ale nebyl ještě dokonalý. Pro pohodlnou komunikaci musela být výměna čísel ke klíči synchronní. Pokud chtějí dvě osoby komunikovat šifrovaně, musí se nejdříve dohodnout na klíči. Pokud by jeden musel čekat s odpovědí na druhého, než by mohl zaslat nějakou zprávu, byla by komunikace nepohodlná. I přes toto bylo toto schéma obrovským skokem dopředu a dovolilo, aby spolu mohly dvě osoby komunikovat, aniž by museli složitě distribuovat klíč. Teď bylo jen nutné vytvořit efektivnější způsob.

Revoluce v šifrování Zatímco Merkel pracoval na své metodě Diffie se snažil najít jiný způsob přenosu. Po čase přišel na způsob, který dnes nazýváme *asymetrické šifrování*. U asynchronního šifrování využíváme dvou klíčů. Jeden veřejný, určený pro šifrování, a jeden soukromý, sloužící pro dešifrování. Osobě chtějící napsat jiné osobě stačilo jen zjistit její veřejný klíč, tím zašifrovat svou zprávu a poslat ji. Od té doby si zprávu nikdo, bez znalosti soukromého klíče, což je jen osoba, které je správa učena, nepřečte. Nutností je pouze matematická provázanost mezi soukromým a veřejným klíčem.

Diffie bohužel navrhl tento způsob komunikace, ale nevěděl jak ji reálně implementovat. Už ale tento návrh byl převratný. Dokázal, aby dva lidé spolu komunikovali pohodlně a asynchronně. V roce 1975 svou myšlenku zveřejnil a další věci se snažili najít funkci, která by byla vhodná pro tuto metodu. Funkce musela být jednosměrná a za určitých podmínek k sobě inverzní.

Za nalezení potřebné funkce se postarali inženýři z MIT Ron Rivest, Leonard Adleman a Adi Shamir. Rivest a Shamir hledali nápady a Adleman se snažil jejich teorie rozvrátit, aby se nezabývali zbytečnými nápady. Takhle to běželo až do roku 1977 kdy Rivesta napadlo možné řešení. Přes noc sepsal celý odborný článek a ten ukázal svým kolegům. Aldeman se snažil najít chybu v Rivestových myšlenkách ale to se mu nepo-

vedlo. Po domluvě pak článek podepsali jmény v pořadí Rivest, Shamir, Aldeman. To pak dalo název RSA, který je asi nejdůležitější v moderní kryptografii.

Zjednodušený popis Rivestovy metody je tento. Vychází z dříve popsané Diffieho funkce. Důležitou součástí je číslo n. To vznikne součinem dvou dostečně velkých, náhodných prvočísel p a q. Kvůli bezpečnosti je důležité, aby tato čísla byla prvočísla. Námi vypočtené číslo je pak veřejným klíčem a p spolu s q jsou soukromé klíče jedné osoby. Silnou stránkou této metody je to že zjistit z p a q číslo n je velice jednoduché. Jedná se o pouhý součin. Ale proces získání prvotních dvou čísel z čísla n je pro dostatečně velké čísla prakticky nemožné. Tento problém se nazývá faktorizace a je velice časově náročný. Pokud chce někdo osobě napsat, použije její veřejný klíč jako exponent v na začátku zmiňované obecné funkci, která je taky veřejná. Výsledné číslo je pak zašifrovaný text a to pošleme druhé osobě, jejíž veřejný klíč jsme použili. Ta osoba pak použije svůj soukromý klíč k dešifrování textu.

RSA řeší všechny předchozí problémy. Není potřeba si tajně předávat klíč komunikace, komunikace může být asynchronní a navíc s dostatečně velkými vstupními klíči je nepřekonatelná. Jako klíč se berou čísla 10^130. Pro důležitější komunikace doporučují klíče nejméně 10^308. Problémem pro tento způsob by bylo, kdyby někdo přišel na způsob jak řešit problém faktorizace. Ten se ale neúspěšně hledá přes 2000 let a mnoho matematiků se domnívá, že z nějaké matematické zákonitosti takové řešení neexistuje.

I když jsou Diffie, Hellman a Merkle považování za vynálezce konceptu šifrování s veřejným klíčem a Rivest, Shamir a Aldeman uznávání za nejlepší implementaci veřejného klíče byly tyto objevy jako první učiněny jinými. Britská armáda měla veliké náklady na distribuci klíče stejně jako ostatní země. Zadali proto vyřešení tohoto úkolu svým nejlepším vědcům. Jamese Ellise pracující v britském GCHQ které bylo následníkem Bletchley Parku, byl jedním z nich. Ihned to stanovil jako svou prioritu a začal hledat radikální řešení.

Po čase strávené hledáním odpovědi přišel ke zprávě od neznámého autora z druhé světové války. Ten navrhoval, že bude skrývat obsah telefonní linky přidáním šumu. Přesné parametry zná pouze on, a tudíž jen on je pak dokáže odstranit. Tím se příjemce zasluhuje o proces šifrování. Tehdy však byl takový nápad nepraktický a těžko realizovatelný.

Ellis tehdy věděl, že je možné umožnit bezpečnou komunikaci bez nutnosti výměny klíče. Přišel taky na myšlenku veřejného a soukromého klíče. Hledal potřebnou jednosměrnou funkci, ale neměl moc znalostí matematiky, tudíž byl u konce svých schopností. Tehdy ukázal svůj objev nadřízeným a ti tento úkol předali jiným. Tři roky nemohl nikdo z GCHQ přijít na řešení. Až v září roku 1973 přišel do GCHQ Cliffords Cocks který byl absolventem Cambridge v oboru teorie čísel. Ten jako matematik problém vyřešil hned poté, co jej zjistil. Už čtyři roky před objevením RSA byla podobná metoda odhalena Cocksem. Ten, stejně jako každý v CGHQ, byl vázán slibem nezveřejnit nic, co se týká jejich práce. Navíc byl nápad objeven v době, kdy ještě nebyly počítače dostatečně výkonné na asymetrické šifrování.

Cocks ukázal tento šifrování s veřejným klíčem svému kamarádovi Malcolmovi Williamsovi, který také pracoval pro CGHQ. Ten se snažil najít na tomto nápadu nějakou

chybu, ale neuspěl. Místo toho přišel na metodu výměny klíče stejnou, jako byla metoda Diffie-Hellman-Merkle.

Britští vědci, na rozdíl od amerických, byli nuceni o svých objevech mlčet. Britové nedokázali docenit hodnot svých objevů. Až roku 1997 odtajnili přínos GCHQ na moderním šifrování a jejím vědcům mohlo být dostáno uznání.

Šifrování pro masy Na konci 80. let se začínal rozvíjet internet Přenos dat a zpráv na něm začalo využívat čím dál více lidí. Jediná tehdejší bezpečná a pohodlná metoda šifrování byla metoda RSA. Ta však byla náročná a vyžadovala dostatečně silný počítač. Těmi, v té době, disponovala pouze vláda, armáda a velké korporace. Na přelomu století navíc nastalo dilema, kdy bylo nutné mít šifrovací systém, kdy obyčejní lidé i firmy mohou mít bezpečnou formu šifrování, ale ta by se nedala zneužít teroristy. Aktivista Philip Zimmerman se snažil zasadit, aby i obyčejní lidé mohou využít bezpečnost, kterou dává RSA. Vymyslel projekt nazvaný Pretty Good Privacay (PGP). Na konci 80. let přišel s balíčkem softwaru. Ten, aby urychlil šifrování, vymyslel proces, kdy se využívá šifra IDEA, která je podobná DES. Aby vyřešil problém distribuce klíče, použil metodu RSA pro zašifrování klíče šifry IDEA. Tím odstranil nutnost šifrovat velké objemy dat pomocí RSA. To přineslo možnost bezpečné komunikace obyčejným lidem.

Dalším přínosem PGP bylo automatické generování klíče RSA a elektronický podpis emailů. Ten je velice důležitý pro ověřování pravosti autora. Je založen na principu popsaném Diffiem a Hellmanem. Byli si vědomi, že jejich systém šifrování se dá využít jak pro vyřešení problému distribuce klíče tak jako mechanismus pro elektronický podpis emailů. U šifrování se využívá veřejný klíč pro šifrování a soukromý pro dešifrování. U elektronického podpisu se tento proces obrátí. Šifruje se soukromým klíčem a dešifruje veřejný. Nezajistí nám to sice bezpečnost emailu, ale jednoznačně určí, kdo ho poslal. Po dešifrování veřejným klíčem určité osoby máme jistotu, že pouze ta osoba jej zašifrovala, protože pouze ona zná odpovídající soukromý klíč.

Zimmerman nevymyslel novou metodu šifrování. Pouze využil už známých postupů a vytvořil software, který celý proces zautomatizoval a ulehčil tak jeho uživatelům práci se zabezpečenou komunikací na obyčejných osobních počítačích.

Nasazení PGP však bránilo, že RSA je patentově chráněný produkt a byla vyžadována licence k jeho využití. Zimmerman však zamýšlel, že cílovou skupinou budou obyčejní lidé, tudíž nebude konkurovat přímo šifře využívající RSA, kterou používaly velké firmy a vláda. Dalším problémem byl nový trestný zákon. Ten přikazoval poskytovatelům služeb elektronické komunikace a objekty vyrábějící vybavení pro takovou komunikaci musí zajistit, aby jejich vybavení dovolilo poskytnout vládním úřadům nezašifrované data jejich komunikace. Chtěli zaručit, že mohou odposlouchávat všechny komunikace.

Zimmerman aby zajistil, že jeho produkt bude zdarma pro všechny lidi, jej roku 1991 veřejně vystavil na internet. Program se po nějaké době rozšířil do celého světa.

Velká rozšířenost PGP se nelíbila dvou subjektům. Jedním byla RSA Data Security, Inc., která nedala Zimmermanovu PGP povolení pro užívání metody RSA a druhou byla

vláda spojených států. V roce 1993 ho obvinili z nelegálního exportu zbraní. Šifrovací techniku totiž kategorizovali stejně jako střelné nebo výbušné zbraně.

V dalších letech probíhala velká diskuze jak přistoupit k šifrování. Zastánci šifrování argumentovali právem na ochranu soukromí. Chtěli, aby se šifrování nijak neomezovalo a nezasahovalo se do něj. Naproti tomu byli lidé, kteří se báli zneužití šifrování teroristy a nelegálními skupinami. To bylo dokonce mnohokrát dokázáno.

Jedním z řešení této situace, bylo vytvoření takzvanou depozici klíčů. Určí se jedna bezpečná a nezávislá osoba, která zná všechny veřejné i neveřejné klíče. Pokud by zjistili, že je někdo zapleten do zločinu poté soukromý klíč té osoby odtajní policii.

Tím by byla zaručena aspoň částečná možnost proniknout do komunikace osob konající trestnou činnost, ale vyžadovalo to svěřit svůj veřejný i soukromý klíč nějaké třetí osobě. Mimo vládu, která tento způsob prosazovala, nebylo moc příznivců takového systému, proto se také tento systém neprosadil.

V roce 1996, tři roky po obžalovaní Zimmermana, stáhli žalobu vedenou proti němu. Zimmermanovi se nepodařilo prokázat přímou vinu a navíc byl program PGP už tak rozšířen, že se stíhání Zimmermana ničeho nedokázalo. PGP pak bylo vyvíjeno nezávislými evropskými vývojáři i americkou společností Network Associates, kde Zimmerman nastoupil jako jeden z vedoucích pracovníků.

Na přelomu tisíciletí byl rozvoj počítačové kryptografie už tak rozšířený, že za nějaký čas všechny země, které šifrování nějak omezovaly, buď zrušily své omezení, nebo je velmi zmírnily.

Šifrovací algoritmy se neustále vyvíjejí a s nimi i kryptoanalýza. Zdálo se, že kryptografie začala mít navrch, ale nově se objevily způsoby útoku na způsob implementace namísto matematické podstaty šifry. Využívá se třeba zkoumání spotřeby elektrické energie elektronických součástek, čas, který je potřebný k šifrování a podobné nepřímé veličiny. Takovým způsobům se říká útok postranními kanály.

V posledních letech bylo prolomeno mnoho šifrovacích standardů, jako byly třeba metody DES a WEP. DES bylo nahrazeno mnohem bezpečnějším AES a místo WEP se používá WPA a ještě, dnes už modernější, WPA2.

3.6 Budoucnost kryptologie

Jako nejperspektivnější obor kryptologie do budoucna je označována kvantová kryptografie. Dnešní algoritmy spoléhají na matematické zákonnosti pro svou bezpečnost. Kvantová kryptologie však využívá vlastnosti kvantové fyziky.

Kvantová kryptologie je založena na využití jednotlivých částic světla, fotonů, a jejich chování. Hlavní vlastnost, která se zde využívá, je že každé měření stavu fotonu tento stav nějak ovlivňuje. Tohoto se dá využít při řešení problému přenosu klíče.

Kvantová kryptologie využívá kvantové počítače. Ten namísto klasických bitů, které mohou nabýt hodnot 1 nebo 0, ale nikoliv zároveň, pracuje s qubity. Ty mohou být v takzvané superpozici jejich hodnota je zároveň 1 i 0. Díky této vlastnosti by bylo možné zpracovávat mnoho stavů najednou a v ohrožení prolomením by byla i šifra RSA.

V dnešní době však nemáme dostatečné znalosti ani technické vybavení na sestavení takového počítače.

4 Šifry

Popis šifer implementovaných v praktické části. Pro lepší pochopení principů šifer jsme omezili abecedu na písmena bez diakritiky od *A* do *Z*.

Informace, použité k vytvoření a sepsání této kapitoly, jsem čerpal z internetových stránek *practicalcryptography.com* [7] a *wikipedie.org* [8].

4.1 Atbaš

Popis Vynalezení této šifry se datuje okolo roku 500 př. n. l. Byla vynalezena Hebrejci a původně se s ní šifrovala hebrejská abeceda, ale dá se využít se všemi abecedami. Její použití můžeme nalézt třeba v Bibli v knize Jeremjáš, kde byl zašifrován název města Babylón.

Atbaš je velice jednoduchá monoalfabetická substituční šifra. Každé písmeno se šifruje podle jejího pořadí v abecedě tak, že první písmeno je zašifrováno na poslední, druhé na předposlední a tak dále. Díky tomu že nemá žádný vstupní klíč potřebný k šifrování a jedná se o monoalfabetickou šifru je nesmírně lehká na prolomení i bez použití pomůcek.

Příklad Jako příklad si zvolíme slovo *ABECEDA*. Postupně budeme šifrovat jednotlivá písmena. Bereme v úvahu klasickou abecedu s 26 znaky.

A > Z Z 1. místa na 26.
B > Y Z 2. na 25.
E > V Z 5. na 22.
C > X Z 3. na 24.
E > V Z 5. na 22.
D > W Z 4. na 23.
A > Z Z 1. na 26

Výsledné slovo vypadá takto: *ZYVXVWZ*

4.2 Caesarova šifra

Šifra používána Juliem Caesarem, který žil od roku 100 př. n. l. do roku 44 př. n. l. Byl jako první zaznamenaný uživatel této šifry. Využíval ji k šifrování vojenských informací, považovala se tudíž na svou dobu za poměrně bezpečnou. Jako klíč si zvolil posunutí o tři pozice. Dále tuto šifru využíval Augustus Caesar, synovec Julia Caesara. Ten využíval posun o jednu pozici. Caesarova šifra bývá označována jako jedna z nejznámějších klasických šifer.

Jedná se o monoalfabetickou substituční šifru s využitím číselného klíče. Funguje na principu posunutí šifrované abecedy oproti původní o konstantní počet pozic daný klíčem. Klíč je podle délky abecedy omezen od 1 do 26, existuje tudíž 25 šifrovaných abeced. Pro svou malou množinu klíčů lze jednoduše použít pro prolomení metodu brute force.

Matematický zápis zašifrování písmene kde n je posun a x je pozice písmene v abecedě:

$$E_n(x) = (x + n) \bmod 26 \tag{2}$$

Příklad Jako klíč si zvolíme posun šifry o 3 pozice. Vstupní slovo bude *ABECEDA*.

Posun o:	0		1		2		3
	A	>	B	>	C	>	D
	B	>	C	>	D	>	E
	E	>	F	>	G	>	H
	C	>	D	>	E	>	F
	E	>	F	>	G	>	H
	D	>	E	>	F	>	G
	A	>	B	>	C	>	D

Výsledný zašifrovaný text vypadá takto: *DEHFHGD*

4.3 Enigma

Enigma byla vynalezena ve firmě Scherbius & Ritter roku 1918. Firma nabízela různé verze určené jak soukromému sektoru, tak vládě. Na svou dobu tento elektromechanický přístroj poskytoval velice bezpečnou šifru, ale byl nesmírně drahý. To odrazovalo potencionální kupce. Firmám se zdálo zbytečné mít tak silnou šifru a pozdější uživatel Enigmy, Německo, ještě nevědělo, že její šifry jsou prolomeny, tudíž nechtělo zbytečně investovat.

Kolem roku 1925 Němci zjistili, že jejich komunikace už není bezpečná a rozhodli se nakoupit přístroje Enigma. Do roku 1945 nakoupili asi 30 000 těchto přístrojů. Využívalo ji ve všech svých úřadech a válečných institucích. Německo mělo na tehdejší dobu nejpokročilejší šifrovací systém a myslelo si, že i to jim pomůže vyhrát 2. světovou válku.

Díky zradě pracovníka v německém kryptologickém úřadě a nesprávnému používání informací byli v polském Biuru Szifrov schopni prolomit jejich šifru. Němci po čase zlepšili bezpečnost Enigmy a šifra byla zase na čas bezpečná.

Za pozdější prolomení se zasloužil hlavně britský Alan Turing. Sestavil mechanický přístroj Bombe který dokázal zjistit nastavení Enigmy v dostatečně krátkém čase. Její prolomení významně přispělo k vítězství spojenců nad Německem.

Enigma je elektromechanický stroj skládající se z několika samostatných součástí. První je klávesnice pro zadávání písmen s 26 znaky klasické abecedy (A - Z). Tři otočné rotory s různým vnitřním propojením, které převádějí jedno písmeno na jiné, reflektor podobný rotorům avšak bez přetáčení, panel s žárovkami který signalizuje výstupní písmeno a baterie. Vojenská verze dále měla propojovací desku, kde můžeme mít až 10 propojení dvou různých písmen. Přístroj funguje na principu uzavření elektrického obvodu.

K zahájení šifrování musíme být Enigma nastavena. Toto nastavení je důležité si zapamatovat pro dešifrování zprávy. Nastaveno může být, jaké typy rotorů se využijí. Vojen-

ská verze, která je implementována v praktické části této bakalářské práce měla k dispozici 5 rotorů. Dále se nastavovala začáteční pozice jednotlivých rotorů a propojení písmen na propojovací desce.

Bohatá možnost nastavení vedla k obrovskému počtu kombinací:

Kombinace rotorů:	$5 \times 4 \times 3$	=	60
Startovní pozice rotorů:	$26 \times 26 \times 26$	=	17 576
Zapojení propojovací desky:	$(26!)/(6! \times 10! \times 2^{10})$	=	150 738 274 937 250
Celkem:		=	158 962 555 217 826 360 000

Po zmáčknutí klávesy na klávesnici se přetočí třetí rotor. Ten, pokud je na pozici k přetočení dalšího, předem určené každému rotoru, podá povel k přetočení druhého. U něj se zase rozhoduje o přetočení prvního rotoru. Impulz z klávesnice poté projde přes propojovací desku, třetí rotor, druhý rotor, první rotor a poté do reflektoru. Od něj prochází impuls zpátky obráceně. Nejdříve první rotor, pak druhý, pak třetí. Následně do propojovací desky a konečně na panel s žárovkami kde rozsvítí výsledné písmeno.

Dešifrování probíhá stejně jako šifrování. Musíme mít nastavenou Enigmu na stejné nastavená, jako bylo použito při šifrování, pak stačí jen postupně zapisovat zašifrovaný text a na výstupu bude text dešifrovaný.

Příklad Zvolme si pro příklad rotory *I*, *II*, *III*. Ty nastavíme na počáteční pozice *Z*, *B* a *V*. Na propojovací desce propojíme písmeno *A* s písmenem *B* a *C* s *X*. Ted' můžeme začít šifrovat vstupní slovo *ABECEDA*.

Na klávesnici zmáčkneme tlačítko *A*. Rotor číslo tři se pootočí na znak *W*. Zkontroluje se, jestli je na pozici kdy se má pootočit druhý rotor. Pro rotor *III* je to písmeno *W*. Druhý rotor se proto pootočí na pozici *C*. Opět se kontroluje pootočení dalšího rotoru. Rotor *II* má jako přetáčecí pozici *F*. První rotor se nepřetáčí. Obvodem začne procházet elektrický proud.

Z tlačítka *A* jde signál na propojovací desku. Jelikož máme propojené písmena *A* a *B*, signál pokračuje na 2. pozici třetího rotoru což je aktuálně *X*. Písmeno *X* je na rotoru *III* propojené s písmenem *S* které je na 18. pozici v abecedě. Jelikož je tento rotor pootočený o 22 pozic napřed, vychází signál na 22. pozici. Druhý rotor je pootočený o 2 pozice. Signál přichází na pozici 24 v abecedě což je písmeno *Y*. Na rotoru *II* je *Y* spojené s *O*. *O* je v abecedě na pozici 14. Se započtením pootočení vychází signál na 12. pozici. První rotor je pootočen o 25 pozic. Signál tedy přijde na písmeno na pozici 11, kterým je *L*. To je v rotoru *I* propojené s *T*. *T* je na 19. pozici a po zahrnutí pootočení vychází signál na 20. pozici.

Z prvního rotoru jde signál na reflektor na 20. pozici kde je písmeno *U*. To je spojené s písmenem *C* které je na 2. pozici. Signál jde zpět na první rotor. Putuje na 2. pozici prvního rotoru, kterým je písmeno *B*. *B* je spojené s *W*. S přetočením vychází signál na 23. pozici. Na druhém rotoru přijde na písmeno *Z* které je spojené s *S* na aktuálně 16. pozici rotoru. Třetí rotor má na 16 pozici písmeno *M*. To je spojené s *V* které je na 25. pozici.

Signál jde na 25 pozici na propojovací desce kde je písmeno *Z*. Jelikož to není propojené s žádným písmenem, signál skončí na žárovce s písmenem *Z*.

Tyhle kroky se opakují pro každé písmeno. Jen se podle písmene mění pozice signálu vstupujícího na propojovací desku.

Další písmena:

B > D
E > X
C > X
E > I
D > R
A > S

Ze slova *ABECEDA* s našim konkrétním nastavením vznikne slovo *ZDXXIRS*. Jako zajímavosti si můžeme všimnout, že dvě různá písmena *E* a *C* se zašifrovaly na stejné písmeno *X* a zároveň obě písmena *E* se zašifrovaly na různá písmena a to *X* a *I*.

4.4 Šifra Playfair

Šifra Playfair byla poprvé popsána roku 1854 Britem Charlesem Wheatstonem. Jedná se o polygrafickou, monoalfabetickou šifru kde se pracuje s bigramy textu. Své jméno nedostala podle svého objevitele ale podle největšího zastánce a propagátora této šifry, Lorda Playfaira.

Byla používána za první i druhé světové války jako rychlá šifra pro zabezpečení málo citlivých údajů, které byly důležité jen na krátký čas. Nesměla být použita na ukrytí zpráv větší důležitosti.

Při šifrování i dešifrování využívá tato šifra upraveného Polybidova čtverce, což je tabulka s pěti sloupci a pěti řadami. Jeho podoba je určena klíčem kdy se jeho písmena zapisují od začátku tabulky, každé pouze jednou. Po vypsání všech písmen klíče dopíšeme do tabulky zbývající písmena abecedy podle abecedního pořadí. Jelikož využíváme 26 znakovou abecedu, musíme vynechat nebo zaměnit jedno písmeno. Nejčastěji se vynechává *Q* nebo se místo písmene *J* píše písmeno *I*.

Tabulky 5×5 dává $25!$ možných kombinací. To je 15 511 210 043 330 985 984 000 000.

Po sestavení tabulky se text rozdělí do dvojic písmen, tzv. bigramů. Pokud je jedna dvojice písmen složena ze stejných znaků, vložíme mezi ně písmeno *X*. Druhé písmeno pak vytvoří dvojici s dalším v pořadí. Pokud má text lichý počet znaků, dopíšeme na konec znak *Z*. Dále pracujeme podle tří základních pravidel souvisejících s pozicí dvojic písmen v tabulce.

1. Pokud je dvojice písmen na stejném řádku, nahradíme je za písmena ležící v tabulce napravo od něj. Pokud je písmeno v posledním sloupci nahradíme jej písmenem z prvního sloupce.

2. Jestli jsou obě písmena ve stejném sloupci, nahrazují se za písmeny přímo pod nimi. Písmeno na posledním řádku nahrazujeme tím na prvním.

3. Když písmena neleží ani na stejném sloupci ani na stejném řádku, nahrazují se za ty ležící na stejném řádku, ale ve sloupci toho druhého písmena ze dvojice.

Dešifrování textu probíhá stejným způsobem jako šifrování. Po dešifrování tabulkou je text mírně změněný kvůli přidání znaků pro rozdělení symetrických bigramů.

Příklad Budeme šifrovat slovo *ABECEDA*. Jako klíč zvolíme slovo *PLAYFAIR*. Nejdřív musíme sestavit tabulku. Budeme postupovat po řádcích.

1. Do pozice na prvním řádku a prvním sloupci napíšeme znak *P*.
2. Do pozice na prvním řádku a druhém sloupci bude znak *L*.
3. Do pozice na prvním řádku a třetím sloupci bude znak *A*.
4. Do pozice na prvním řádku a čtvrtém sloupci bude znak *Y*.
5. Do pozice na prvním řádku a pátém sloupci bude znak *F*.
6. Do pozice na druhém řádku a prvním sloupci bude znak *I*. Znak *A* už v tabulce jednou je.
7. Do pozice na druhém řádku a druhém sloupci bude znak *R*.
8. Dále vypíšeme všechny zbývající písmena abecedy, které ještě v tabulce nejsou. Nesmíme zapomenout vynechat písmeno *J* nebo *Q*.

Výsledná tabulka:

	1	2	3	4	5
1	P	L	A	Y	F
2	I	R	B	C	D
3	E	G	H	K	M
4	N	O	Q	S	T
5	U	V	W	X	Z

Dále si rozdělíme vstupní text do dvojic: AB EC ED AZ Protože byl text lichý, dopsali jsme na konec písmeno *Z*.

Můžeme začít šifrovat.

1. Řešíme dvojici *AB*.
   - *A* je na pozici 1,3. *B* je na pozici 2,3.
   - Obě písmena mají stejné sloupce. Tuhle situaci řešíme podle pravidla 2.
   - Písmeno *A* se změní na písmeno *B*. Písmeno *B* se změní na *H*.
   - Výslednou dvojici *BH* zapíšeme na výstup.
2. Dvojice *EC*

- *E* je na pozici 3,1. *C* je na pozici 2,4.
- Nejsou stejné ani řádky ani sloupce. Použijeme pravidlo 3.
- Písmeno *E* se změní na *K*. Písmeno *C* se změní na *I*.
- Výslednou dvojici *KI* zapíšeme na výstup.

3. Dvojice *ED*
   - *E* je na pozici 3,1. *D* je na pozici 2,5.
   - Nejsou stejné ani řádky ani sloupce. Použijeme pravidlo 3.
   - Písmeno *E* se změní na *M*. Písmeno *D* se změní na *I*.
   - Výslednou dvojici *MI* zapíšeme na výstup.
4. Dvojice *AZ*
   - *A* je na pozici 1,3. *Z* je na pozici 5,5.
   - Nejsou stejné ani řádky ani sloupce. Použijeme pravidlo 3.
   - Písmeno *A* se změní na *F*. Písmeno *Z* se změní na *W*.
   - Výslednou dvojici *FW* zapíšeme na výstup.

Slovo *ABECEDA* se změnilo na slovo *BHKIMIFW*.

4.5 Šifra Rail Fence

Transpoziční šifra, jež dostala jméno podle způsobu zapisování textu. Klíčem určíme počet kolejí, do kterých poté zapisujeme vstupní text způsobem, kde první písmeno zapíšeme na prví řádek, druhé na druhý, a tak pokračujeme dokud nenarazíme na poslední kolej. Poté začínáme písmena zapisovat vzestupně až do první koleje. Poté se opakuje sestupné zapisování. Po zapsání všech písmen čteme text po řádcích.

Příklad Zvolíme si 3 koleje a šifrovat budeme slovo *ABECEDA*. Budeme postupně zapisovat písmena do kolejí.

1. *A* zapíšeme na 1. kolej.
2. *B* zapíšeme na 2. kolej.
3. *E* zapíšeme na 3. kolej.
4. *C* zapíšeme na 2. kolej.
5. *E* zapíšeme na 1. kolej.
6. *D* zapíšeme na 2. kolej.
7. *A* zapíšeme na 3. kolej.

První kolej obsahuje písmena *AE*. Druhá kolej obsahuje písmena *BCD*. Třetí kolej obsahuje písmena *EA*. Po spojení dostaneme výsledné slovo *AEBCDEA*

4.6 Sloupcová šifra

Další druhem transpoziční šifry je sloupcová šifra nebo také sloupcová transpozice. Slovním klíčem určíme počet sloupců, do kterých zapíšeme vstupní text. Poté vypisujeme sloupce podle pořadí písmene odpovídajícího sloupce od začátku abecedy.

Vylepšenou variantu této šifry, dvojitou transpozici, kde se transpoziční šifra aplikovala dvakrát za sebou, používalo Německo za první světové války jako rychlou a jednoduchou šifru na bojišti.

Příklad Klíčem bude slovo *PES* a šifrovat budeme slovo *ABECEDA*.

Sestavíme tabulku o velikosti klíče a vepíšeme do ní slovo, které chceme šifrovat.

P	E	S
A	B	E
C	E	D
A		

Poté si ohodnotíme sloupce podle písmene klíče. Nejdříve v abecedě je písmeno *E*, dále *P* a nakonec *S*. Podle ohodnocení vypíšeme druhý sloupec, pak první a nakonec třetí. Výsledné slovo je *BEACAED*.

4.7 Jednoduchá substituční šifra

Velice jednoduchá šifra, která mění písmena z otevřeného textu na zašifrovaný podle předem navolených substitucí. Tím vytvoříme takzvanou *substituční abecedu*. Absence pravidel této šifry nám dává možnost nasimulovat jakoukoliv monoalfabetickou šifru. Můžeme třeba převrátit pořadí písmen v abecedě a tím získáme šifru Atbaš.

I přes to že má tato šifra *26!* možných klíčů není velmi bezpečná. Jedná se o monoalfabetickou šifru a s dostatečně dlouhým zašifrovaným textem lze zjistit klíč poměrně snadno.

Příklad Vstupní slovo je *ABECEDA*. Teď si musíme nastavit substituce. Zvolíme si:

- A - N
- B - C
- D - P
- H - R

Postupujeme po písmenech a hledáme, jestli je písmeno v našich zvolených substitucích.

1. *A* je v substitucích. Změníme jej na *N*.
2. *B* je v substitucích. Změníme jej na *C*.

3. *E* není v substitucích. Písmeno *E* zůstává.
4. *C* je v substitucích. Změníme jej na *B*.
5. *E* není v substitucích. Písmeno *E* zůstává.
6. *D* je v substitucích. Změníme jej na *P*.
7. *A* je v substitucích. Změníme jej na *N*.

Slovo *ABECEDA* se s našimi zvolenými substitucemi změnilo na *NCEBEPN*.

4.8 Vernamova šifra

V roce 1917 Gilbert Vernam vynalezl a nechal si patentovat nový druh polyalfabetické proudové šifry. Jednalo se o postup, kdy se každý znak v otevřeném textu zašifruje s odpovídajícím znakem ze vstupního klíče, který je stejně dlouhý jako otevřený text, podle součtu jejich pořadí v abecedě. Tento typ šifry popsal už roku 1882 Frank Miller, ale tehdy se nápad nerozšířil. Pro dokonalou bezpečnost musí být klíč naprosto náhodný a navíc nelze použitý klíč nikdy opakovat. To je vcelku jednoduché, protože N znaků dlouhý vstupní text má 26^N možných klíčů.

Roku 1949 C. E. Shannon matematický dokázal, že tato šifra je naprosto neprolomitelná. Musí se však zajistit náhodnost klíče, jeho délka a to že klíč nesmí být použitý k šifrování více než jedné zprávy. Shannon ukázal, že zašifrovaná zpráva neobsahuje žádné informace o vstupním textu. Šifra se nedá rozlišit od náhodné posloupnosti znaků a není tedy možné ji prolomit.

Existuje i binární varianta Vernamovy šifry která využívá funkce XOR a tou kombinuje jednotlivé bity klíče s bity vstupního textu.

Tato šifra je sice velice bezpečná, ale kvůli nárokům na klíč vhodná jen pro komunikaci kdy je bezpečnost největší prioritou a pro její zachování je možné vynaložit hodně prostředků. Používá se třeba pro komunikaci mezi prezidentem USA a Ruska, která je známá jako horká linka.

Příklad Budeme opět šifrovat slovo *ABECEDA*. Nejdříve je nutné najít si vygenerovat heslo stejné délky. Pro příklad si zvolíme heslo takto: *WFPDROB*.

1. Písmeno *A* je na 0. pozici a *W* je na 22. pozici. $0 + 22 = 22$ Vyjde nám písmeno na 22 pozici což je *W*.
2. Písmeno *B* je na 1. pozici a *F* je na 5. pozici. $1 + 5 = 6$ Na 6. pozici je *G*.
3. Písmeno *E* je na 4. pozici a *P* je na 15. pozici. $4 + 15 = 19$ Na 19. pozici je *T*.
4. Písmeno *C* je na 2. pozici a *D* je na 3. pozici. $2 + 3 = 5$ Na 5. pozici je *F*.
5. Písmeno *E* je na 4. pozici a *R* je na 17. pozici. $4 + 17 = 21$ Na 21. pozici je *V*.

6. Písmeno *D* je na 3. pozici a *O* je na 14. pozici. $3 + 14 = 17$ Na 17. pozici je *R*.

7. Písmeno *A* je na 1. pozici a *B* je na 1. pozici. $1 + 1 = 2$ Na 2. pozici je *B*.

Ze slova *ABECEDA* se stalo *WGTFVRB*.

4.9 Vigenerova šifra

Šifra vycházející z nápadu Leona Battisty Albertiho použít více šifrovaných abeced pro jeden otevřený text. Alberti svou šifru zveřejnil roku 1467, ale až roku 1553 Giovan Battista Bellaso dokončil jeho myšlenku a vznikla tato šifra, jak jí známe dnes. Její jméno je podle Blaise de Vigenera, kterému bylo objevení nesprávně přiřazeno.

Ve své době se této šifře přezdívalo *Le chiffre indechiffrable*, tedy nerozluštitelná šifra. Využívá 26 šifrovaných abeced, které se přiřazují podle vstupního klíče. Tím je slovo, které se periodicky zapíše pod otevřený text a podle Vigenerova čtverce, což je tabulka s vypsanými všemi šifrovacími abecedami, vypisujeme zašifrovaný text. Podle délky klíče taky určujeme bezpečnost šifry. Problémem je totiž periodicita, s kterou se klíč opakuje. Využitím této slabiny lze šifru jednoduše překonat.

Jako první na tuto metodu přišel Charles Babbage, který ji však nezveřejnil. Poté byla nezávisle na něm objevena Friedrichem Kasiskim. Podle něj je taky pojmenována. Jde o metodu kde hledáme opakující se části textu. To nám dává možnost odhadnout délku klíče a tím šifru rozdělit na více jednodušších monoalfabetických šifer které už lehce zvládneme prolomit.

Příklad Vstupní slovem bude *ABECEDA* a klíč *PES*. Napíšeme si klíč nad slovo k zašifrování. Podle potřeby klíč opakujeme.

P	E	S	P	E	S	P
A	B	E	C	E	D	A

Dále kombinujeme jako u Vernamovy šifry.

1. Písmeno *A* je na 0. pozici a *P* je na 15. pozici. $0 + 15 = 15$ Vyjde nám písmeno na 15 pozici což je *P*.

2. Písmeno *B* je na 1. pozici a *E* je na 4. pozici. $1 + 4 = 5$ Na 5. pozici je *F*.

3. Písmeno *E* je na 4. pozici a *S* je na 18. pozici. $4 + 18 = 22$ Na 22. pozici je *W*.

4. Písmeno *C* je na 2. pozici a *P* je na 15. pozici. $2 + 15 = 17$ Na 17. pozici je *R*.

5. Písmeno *E* je na 4. pozici a *E* je na 4. pozici. $4 + 4 = 8$ Na 8. pozici je *I*.

6. Písmeno *D* je na 3. pozici a *S* je na 18. pozici. $3 + 18 = 21$ Na 21. pozici je *V*.

7. Písmeno *A* je na 1. pozici a *P* je na 15. pozici. $1 + 15 = 16$ Na 16. pozici je *P*.

Výsledné slovo s klíčem *PES* je *PFWRIVP*. Můžeme si všimnout, že písmena *A* jsou zašifrovaná stejným písmenem a vyjdou obě stejně. To je taky problém který se dá u Vigenerovy šifry využít k jejímu prolomení.

5 Kryptoanalytické algoritmy

Popis kryptoanalytických algoritmů použitých v praktické části. Informace k použitým algoritmům jsem čerpal z internetových stránek *matematika.cz* [4, 5, 6].

5.1 Frekvenční analýza

Frekvenční analýza je jeden z hlavních a nejstarších nástrojů kryptoanalýzy klasických šifer. Byl objeven už Al-Kindim v 9. století. V Evropě se však začal používat až v 15. století v období Renesance.

Tato metoda využívá vlastnosti jazyka, že každé písmeno má určitou pravděpodobnost výskytu v textu. Pokud analyzujeme dostatečné množství textu, dostaneme statistickou frekvenci písmen v daném jazyce. Dá se využít i frekvence dvojic, trojic i více početných skupin písmen. Frekvence se liší podle druhu textu. Vědecké budou mít mírně jiné frekvence než v literatuře a podobně. Není důležité zjistit úplně přesné hodnoty ale spíše co nejbližší.

Pokud víme frekvence daného jazyka, můžeme zjistit, pokud je nějaký text textem toho jazyka. Pokud nám frekvence vyjdou velice podobně, můžeme říct, že se jedná o stejný jazyk.

Nejvíce účinná je tato metoda u prolomení monoalfabetických substitučních šifer. U nich je rozložení frekvencí stejné, jen se mění, u kterých písmen jsou.

Naproti tomu jsou homofonní a polyalfabetické složité na prolomení pouze frekvenční analýzou. Byly vynalezeny právě za účelem odolnosti proti této metodě. Jejich rozložení frekvencí je oproti vstupnímu textu změněno na stejnoměrnější.

5.2 Index koincidence

Další významnou metodou, která pomáhá kryptoanalytikům, je index koincidence. Ten byl vynalezen Williamem F. Friedmanem. Je to index, který vypočítáme nad textem a ten nám řekne jak uniformní tento text je, neboli jak je pravděpodobné že vybereme dvě písmena z textu a tyto písmena budou stejné.

Vypočteme jej takto:

$$IK = \frac{\sum_{x=A}^{x=Z} nx(nx-1)}{N(N-1)} \tag{3}$$

kde n_x je počet výskytu písmene *i* (jdoucí od písmene *A* do písmene *Z*) v textu a *N* je celkový počet znaků.

Pro dokonale stejnoměrně rozvržený text je index koincidence roven $\frac{1}{26}$ což je 0.0385. Pro český text je index okolo 0.06.

Index koincidence se velmi často využívá k určení, zdali je text šifrovaný monoalfabetickou nebo polyalfabetickou šifrou. Monoalfabetická šifra nemění frekvenci rozložení a tím zůstává index stejný jako index původního textu.

5.3 Prolomení Caesarovy šifry

Díky malému počtu klíčů, kterých je v Caesarově šifře 25, lze využít k prolomení metodu útoku hrubou silou. Postupně zkoušíme dešifrovat vstupní text všemi možnými klíči a výstupní text ohodnocujeme frekvenční analýzou. Po vyzkoušení všech klíčů vybereme ten, který měl nejlepší ohodnocení, a vrátíme ho.

5.4 Prolomení Vigenerovy šifry

U prolomení Vigenerovy šifry využívám odhadu délky klíče a jeho periodicity. Určíme si dolní a horní hranici délky odhadovaného klíče.

Poté postupně zkoušíme délky klíč v našem odhadovaném rozmezí. Pro každou délku rozložíme vstupní text na stejný počet textů tak, že první písmeno jde do první skupiny, druhé do druhé skupiny a tak se to opakuje, dokud nedojdeme k číslu délky klíče. Další písmeno pak patří zase do první skupiny, další do druhé a takto text rozložíme až do konce. Třeba pro klíč délky 3 by v první skupině byla písmena 1,4,7,..., v druhé skupině by byla písmena 2,5,8,... a v třetí skupině 3,6,9,....

Po rozdělení do skupin písmen každou skupinu prolomíme jako Caesarovu šifru a pak tyto klíče spojíme a převedeme na slovo. Až získáme klíč ke každé délce klíče z našeho rozmezí, dešifrujeme text podle těchto klíčů. Výsledné texty pak ohodnotíme frekvenční analýzou a klíč k textu s nejlepším ohodnocením pak vrátíme.

6 Program k demonstraci kryptologických algoritmů

Program jsem vytvářel ve vývojovém prostředí Visual Studio 2010 a jako programovací jazyk jsem použil jazyk C#. Podle zásad objektového programování jsem program rozdělil na dvě části. Jednou je knihovna DLL, která obstarává logiku šifrování, dešifrování a kryptoanalýzy, a druhou částí je ukázková Windows Forms aplikace s uživatelským rozhraním využívající dříve zmíněnou knihovnu.

6.1 Kryptografie

Všechny třídy šifer dědí z abstraktní třídy *Cipher*. Využitím polymorfismu jsme zjednodušili implementaci šifer a zajistili konzistenci v jejich používání. Pro nastavení klíče nebo dalších potřebných údajů pro šifrování využíváme konstruktor, kde tyto údaje pošleme jako parametr a vytvoříme si instanci šifry. Tato instance pak pracuje se zadanými parametry.

Třídní diagram sekce kryptografie (viz obr. 6).

Cipher Abstraktní třída, která obstarává převod vstupního textu pro šifrování nebo dešifrování z datového typu *string* na pole *integerů* a předává jej obslužné abstraktní metodě, která jej dále zpracovává.

Významné metody a atributy:

- Abstraktní metoda *encrypt*. Musí být implementována po dědění.
- Abstraktní meroda *decrypt*. Musí být implementována po dědění.
- Metoda *Encrypt* (viz výpis 1). Přijímá text (*string*), pomocí třídy *Util* (viz sekce 6.3) jej převede na pole čísel a předá jej metodě *encrypt* pro další zpracování. Po vrácení hodnot z metody *encrypt* převede pole čísel pomocí třídy *Util* na text (*string*) a vrátí.
- Metoda *Decrypt*. Stejná funkce jako u metody *Encrypt*, pouze obstarává dešifrování.

```
public string Encrypt(string inputText)
{
    return Util.Util.IntToString(encrypt(Util.Util.StringToInt(inputText)));
}
```

Výpis 1: Metoda pro zahájení šifrování.

Atbash Třída šifry Atbaš. Obstarává logiku práce při šifrování a dešifrování pomocí této šifry.

Významné metody a atributy:

- Metoda *encrypt*. Zašifruje vstupní text.
- Metoda *decrypt*. Dešifruje vstupní text.

Caesar Třída Caesarovy šifry.
Významné metody a atributy:

- Atribut *shift*. Vyjadřuje posun šifrované abecedy oproti otevřenému textu.
- Konstruktor. Pomocí parametru *shift* nastavujeme posun šifry.
- Metoda *encrypt* (viz výpis 2). Zašifruje vstupní text.
- Metoda *decrypt*. Dešifruje vstupní text.

```
protected override int[] encrypt(int [] input)
  {
      int [] output = new int[input.Length];
      for (int i = 0; i < input.Length; i++)
      {
          output[i] = (input[i] + this.shift) % Util.Util.ALPHABETH_LENGTH;

      }
      return output;
  }
```

Výpis 2: Implementace šifrovacího algoritmu Caesarovy šifry.

Column Třída sloupcové šifry.
Významné metody a atributy:

- Atribut *key*. Pole čísel vyjadřující vstupní klíč šifry.
- Konstruktor. Nastavuje vstupním slovem klíč šifry.
- Metoda *encrypt*. Zašifruje vstupní text.
- Metoda *decrypt*. Dešifruje vstupní text.

Enigma, Plugboard, Reflector, AbstractRotor a Rotor1 - Rotor5 Třídy obstarávající šifrovací stroj Enigma. Hlavní třídou je třída *Enigma*. Třídou *Plugboard* je implementována propojovací deska Enigmy. Třídou *Reflector* je implementován reflektor Enigmy. Rotory jsou implementovány abstraktní třídou *AbstractRotor*. Ta zajišťuje logiku rotorů. Z této třídy pak dědí třídy *Rotor1* až *Rotor5*. Tyto třídy přijímají všechny metody třídy *AbstractRotor* a rozlišuje je pouze nastavení propojení uvnitř rotorů.
Významné metody a atributy třídy *Enigma*:

- Atribut *rotors*. Pole s aktuálními rotory.
- Atribut *plugboard*. Odkaz na instanci třídy *Plugboard*.
- Atribut *reflector*. Odkaz na instanci třídy *Reflector*.

- Konstruktor. Jako parametry dostává typy rotorů, pootočení rotorů a propoje na propojovací desce. S předanými parametry pak vytváří instance vybraných rotorů a propojovací desky.
- Metoda *rotate*. Řeší kaskádové otáčení rotorů.
- Metoda *encrypt*. Šifruje vstupní text.

Významné metody a atributy třídy *Plugboard*:

- Atribut *connections*. Slovník uchovávající propoje dvou písmen na propojovací desce.
- Metoda *GetPosition* (viz výpis 3). Obstarává logiku průchodu signálu propojovací deskou.

```
public int GetPosition(int inputPos)
  {
      foreach (KeyValuePair<int, int> x in this.connections)
      {
          if (x.Value == inputPos)
          {
              return x.Key;
          }
          else if (x.Key == inputPos)
          {
              return x.Value;
          }
      }
      return inputPos;
  }
```

Výpis 3: Metoda obstarávající průchod signálu propojovací deskou.

Významné metody a atributy třídy *Reflector*:

- Atribut *shiftedAlphabet*. Pole s uloženými převody v reflektoru.
- Metoda *GetPosition*. Obstarává průchod signálu reflektorem.

Významné metody a atributy třídy *AbstractRotor*:

- Atribut *shiftedAlphabet*. Pole čísel vyjadřující přepojenou abecedou rotoru. Nastavuje se při vytváření instance potomka.
- Atribut *rotations*. Aktuální počet přetočení rotoru.
- Atribut *turnoverPosition*. Vyjádření znaku, při kterém dává rotor povel k přetočení dalšího. Nastavuje se při vytváření instance potomka.
- Metoda *Rotate* (viz výpis 4). Obstarává pootočení rotoru.
- Metoda *GetPositionOut*. Obstarává průchod signálu rotorem zpět.

- Metoda *GetPositionIn*. Obstarává průchod signálu rotorem vpřed.

```
public bool Rotate()
  {
      this.rotations = (this.rotations + 1) % Util.Util.ALPHABETH_LENGTH;
      return (this.rotations == this.turnoverPosition);
  }
```

Výpis 4: Metoda k obsluze přetočení rotoru.

Playfair Třída šifry Playfair.
Významné metody a atributy třídy:

- Atribut *key*. Pole čísel vyjadřující klíč šifry.
- Konstruktor. Nastavujeme jim klíč šifry a znaky potřebné k řešení symetrických bigramů, vynechávání znak a konečného znaku.
- Metoda *encrypt*. Zajišťuje úpravu textu a zašifrování podle Polybiova čtverce a pravidel šifry.
- Metoda *decrypt*. Zajišťuje dešifrování podle Polybiova čtverce a pravidel šifry. Očekává validní zašifrovaný text šifrou Playfair.
- Metoda *getPolybiusSquare*. Vrací Polybiův čtverec sestavený podle vstupního klíče šifry.
- Metoda *findCoords*. Zjišťuje souřadnice hledaného znaku v daném Polybiovu čtverci.

RailFence Třída šifry RailFence.
Významné metody a atributy třídy:

- Atribut *railsCount*. Vyjadřuje počet řádků šifry.
- Metoda *encrypt*. Zašifruje vstupní text.
- Metoda *decrypt*. Dešifruje vstupní text.

SimpleSub Třída jednoduché substituční šifry.
Významné metody a atributy třídy:

- Atribut *table*. Pole čísel zaznamenávající jednotlivé posuny písmen.
- Metoda *encrypt*. Zašifruje vstupní text.
- Metoda *decrypt*. Dešifruje vstupní text.

Vernam Třída Vernamovy šifry.
Významné metody a atributy třídy:

- Atribut *key*. Pole čísel vyjadřující klíč šifry.
- Metoda *GenerateKey*. Generuje klíč potřebné délky.
- Metoda *encrypt* (viz výpis 5). Zašifruje vstupní text.
- Metoda *decrypt*. Dešifruje vstupní text.

```
protected override int[] encrypt(int [] input)
  {
      int [] output = new int[input.Length];
      for (int i = 0; i < input.Length; i++)
      {
          output[i] = (key[i] + input[i]) % Util. Util .ALPHABETH_LENGTH;
      }
      return output;
  }
```

Výpis 5: Metoda obstarávající zašifrování textu Vernamovou šifrou.

Vigener Třída Vigenerovy šifry.
Významné metody a atributy třídy:

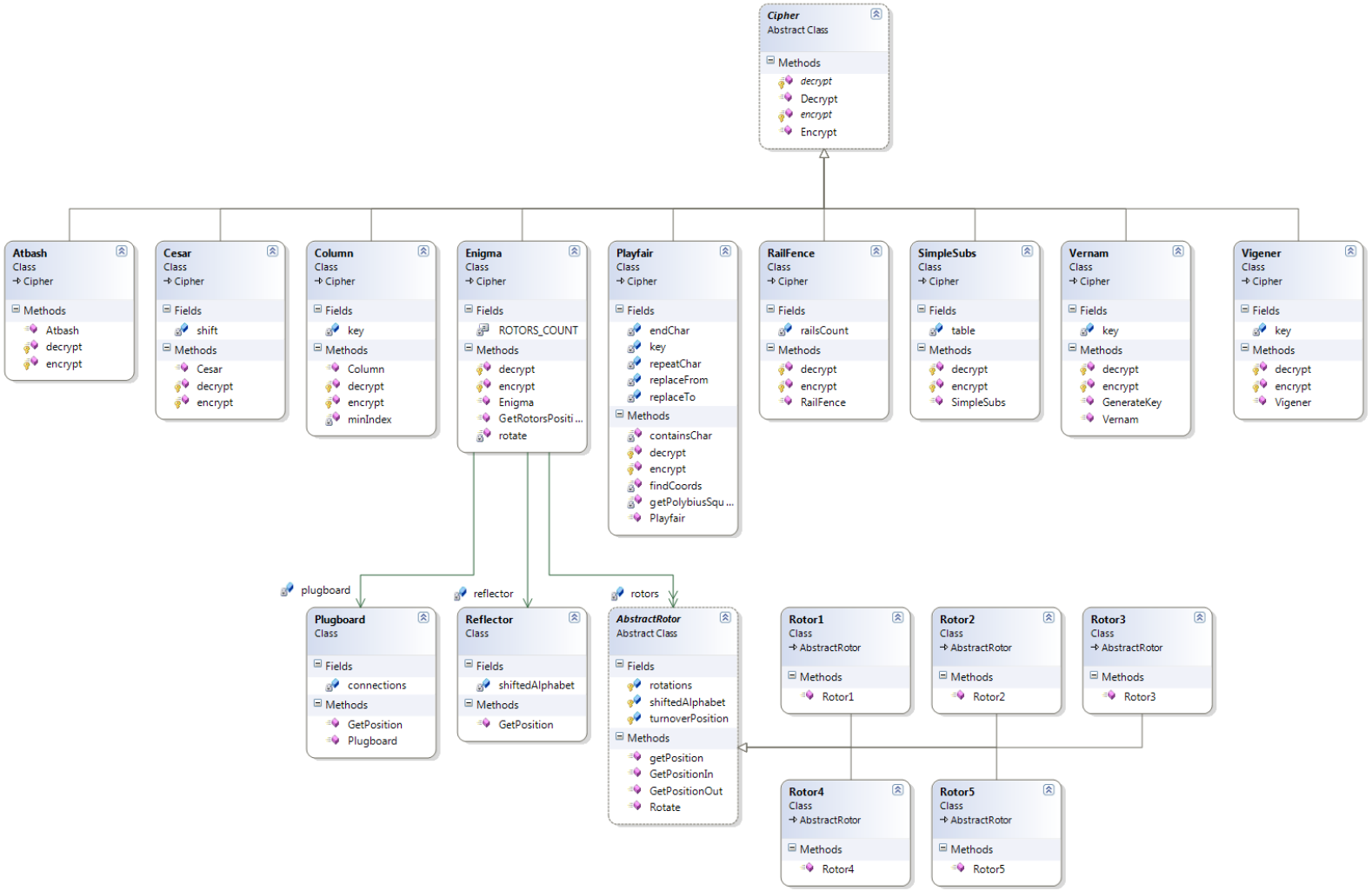
- Atribut *key*. Pole čísel vyjadřující klíč šifry.
- Metoda *encrypt*. Zašifruje vstupní text.
- Metoda *decrypt*. Dešifruje vstupní text.

6.2 Kryptoanalýza

Skupina tříd sloužící ke kryptoanalýze zašifrovaného textu.
Třídní diagram (viz obr. 7).

CaesarBruteFreq Třída řešící prolomení Caesarovy šifry pomocí metody útoku hrubou silou a frekvenční analýzy. Postupně zkouší dešifrovat vstupní text podle všech možných klíčů a tento text ohodnocuje frekvenční analýzou. Poté vybere nejvhodnější text a vrátí odpovídající klíč. Pro správnou funkci je vyžadováno, aby vstupní text byl textem českého jazyka zašifrovaný Caesarovou šifrou.
Významné metody a atributy třídy:

- Metoda *Analyze*. Metoda k zjištění nejvhodnějšího klíč zašifrovaného textu.
- Metoda *shiftChars*. Metoda k další iteraci Caesarovy šifry.
- Metoda *minIndex*. Pomocná metoda k zjištění indexu nejmenšího prvku daného pole.



Obrázek 6: Třídní diagram kryptografie

CoincidenceIndex Třída k zjištění indexu koincidence vstupního textu vůči českému jazyku.

Významné metody a atributy třídy:

- Metoda *Analyze* (viz výpis 6). Vypočte index koincidence vstupního textu.

```
protected override int[] encrypt(int [] input)
  {
      int [] output = new int[input.Length];
      for (int i = 0; i < input.Length; i++)
      {
          output[i] = (key[i] + input[i]) % Util. Util .ALPHABETH_LENGTH;
      }
      return output;
  }
```

Výpis 6: Metoda k zjištění indexu koincidence textu.

FrequencyAnalysis Třída k zjištění frekvence písmen v textu a odchylky textu od rozložení v českém jazyce.

Významné metody a atributy třídy:

- Metoda *Analyze* (viz výpis 7) Metoda vracející odchylku statistického rozložení písmen ve vstupním textu od rozložení písmen v českém jazyce.
- Metoda *GetFrequencies*. Metoda k zjištění frekvence výskytu všech písmen v textu.

```
public double Analyze()
  {
      double[] charsFrequency = GetFrequencies();
      double[] charsDivergence = new double[Util.Util.ALPHABETH_LENGTH];
      for (int i = 0; i < Util . Util .ALPHABETH_LENGTH; i++)
      {
          charsDivergence[i] = Math.Pow((Util. Util . StatisticalDistributionRelativeCzech [i]
              - charsFrequency[i]), 2);
      }
      double tmp = charsDivergence.Sum();
      double tmp1 = charsDivergence.Sum() / (double)text.Length;
      return Math.Sqrt(charsDivergence.Sum() / (double)text.Length);
  }
```

Výpis 7: Metoda k zjištění odchylky rozložení písmen v textu od rozložení v českém jazyce.

VigenerGuessKey Třída prolamující text zašifrovaný Vigenerovou šifrou. Využívá hádání délky klíče k rozdělení zašifrovaného textu polyalfabetickou šifrou na více monoalfabetických a ty jednotlivě zkouší prolomit jako Caesarovu šifru. Pro správnou funkci je vyžadováno, aby vstupní text byl textem českého jazyka zašifrovaný Vigenerovou šifrou.

Významné metody a atributy třídy:

- Metoda *Analyze*. Metoda hledající nejlepší klíč zašifrovaného textu.

6.3 Pomocná třída

Util Tato pomocná třída vznikla, protože v kryptografické a kryptoanalytické části pracují šifry a kryptoanalytické algoritmy místo s písmeny a řetězci písmen s jejich číselným vyjádřením. Čísla jsem přiřadil podle jejich pozice v abecedě a to tak, že $A = 0$, $B = 1$, až po $Z = 25$. V této třídě jsou implementovány všechny potřebné metody a atributy pro převedení z textu nebo písmene na odpovídající čísla a zpět.

Očekáváme validní vstupní text, který se skládá pouze ze znaků *a* až *z* a *A* až *Z* bez diakritiky. Nejsou povoleny čísla, mezery a jiné znaky.

Tato třída také obsahuje další pomocné atributy jako třeba rozložení frekvence výskytu písmen v českém jazyce.

Třídní diagram viz obr. 7.

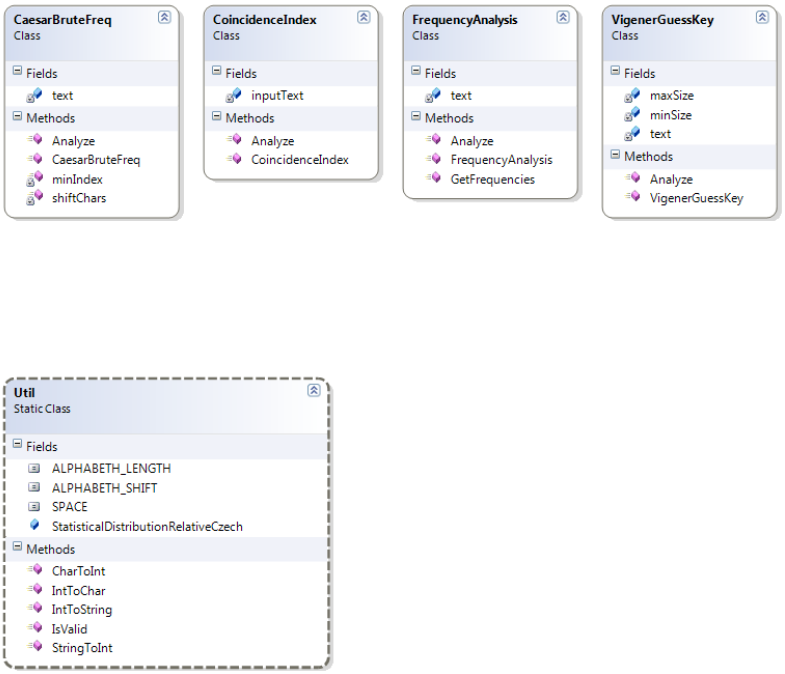
Významné metody a atributy:

- Konstanta *ALPHABETH_SHIFT*. Má hodnotu 65, což je pozice prvního písmene v ASCII tabulce.
- Konstanta *ALPHABET_LENGTH*. Má hodnotu 26, která značí počet znaků abecedy.
- Atribut *StatisticalDistributionRelativeCzech*. Uchovává rozložení frekvencí výskytu písmen v českém jazyce. Tyto hodnoty jsem převzal z webu *matematika.cz* [4].
- Metoda *IntToString* (viz výpis 8). Využíváme ji pro převod pole typu *integer* na typ *string*. Parametrem je text v podobě pole čísel a výstupem je odpovídající řetězec písmen. Pro lepší efektivitu využíváme třídy *StringBuilder*.
- Metoda *StringToInt* (viz výpis 9). Slouží k převodu datového typu *string* na typ pole *integeru*. Jako vstupní parametr má text v podobě řetězce písmen a vrací nám tento text převedený na pole čísel.

```
StringBuilder sb = new StringBuilder();
    for (int i = 0; i < inputNumbers.Length; i++)
    {
        sb.Append((char)(inputNumbers[i] + Util.ALPHABETH_SHIFT));
    }
    return sb.ToString();
```

Výpis 8: Metoda pro převod pole čísel na text.

```
public static int[] StringToInt(string inputText)
  {
      int[] inputNumbers = new int[inputText.Length];
      string inputUpper = inputText.ToUpper();
      for (int i = 0; i < inputText.Length; i++)
      {
          inputNumbers[i] = inputUpper[i] - Util.ALPHABETH_SHIFT;
      }
      return inputNumbers;
  }
```



Obrázek 7: Třídní diagram kryptoanalýzy a pomocné třídy

Výpis 9: Metoda pro převod textu na pole čísel.

6.4 Demonstrační uživatelské rozhraní

Pro testovací potřeby jsem dále vytvořil uživatelské prostředí pro vyzkoušení šifrování, dešifrování a kryptoanalýzy. Toto prostředí je implementováno pomocí Windows Forms aplikace a pro logiku využívá knihovnu s implementovanými šiframi. Ke spuštění této aplikace je nutné mít na počítači nainstalován .NET framework verze 3.5, nebo novější. Jeho popis a práce s ním je detailně popsána v příloze A.

7 Závěr

Hlavním cílem této práce je seznámit čtenáře s historií kryptologie, její strukturou a popsat vybrané kryptografické a kryptoanalytické algoritmy. Navzdory tomu, že toto téma je v době s rozvojem posílání důležitých dat přes internet stále aktuálnější, není mu věnována dostatečná pozornost. V praktické části je pak cílem implementovat algoritmy z teoretické části práce a vytvořit pro ně ukázkové uživatelské prostředí pro jejich otestování.

V teoretické části jsem se zaměřil na seznámení čtenáře se základy kryptologie a jejich podoborů kryptografie, kryptoanalýzy a steganografie. Popsal jsem jejich rozdělení a vysvětlil všechny důležité pojmy, které může čtenář k tomuto oboru potřebovat. Dále jsem popsal historii kryptologie rozdělenou na důležité úseky od jejich raných dob ve starověkém Egyptě, přes její bouřlivý rozvoj v období kolem světových válek až po moderní dobu počítačů. V každém časovém úseku jsem vyzdvihl nejvýznamnější osobnosti té doby, které přispěly do oboru kryptologie nebo jej významně změnily.

U vybraných kryptografických a kryptoanalytických algoritmů jsem popsal jejich fungování a u každého uvedl konkrétní příklad při jejich použití.

V praktické části jsem všechnu potřebnou logiku těchto vybraných algoritmů implementoval v dynamické knihovně se zaměřením na jednoduché další rozšíření s použitím koncepce objektově orientovaného programování. Tato knihovna je plně okomentována a může být využita v různých projektech. Pro demonstraci této knihovny jsem vytvořil testovací uživatelské rozhraní, kde lze všechny implementované algoritmy vyzkoušet a porovnat jejich výstup.

Práce by se dala rozšířit o popis dalších kryptologických algoritmů a jejich následnou implementací. Dále by mohlo být vyvinuty různé typy aplikací využívající mou knihovnu s algoritmy, které by mohly sloužit studijním účelům.

Další možnost pokračování práce je třeba zaměření studia na popis dnes používaných algoritmů a způsobu komunikace, se kterými se využívají.

8 Reference

[1] Piper, Fred - Murphy, Sean *Kryptografie: Průvodce pro každého* Přeložil: Mondschein, Pavel. Praha: Dokořán, 2006. 157 s. ISBN 80-7363-074-5

[2] Singh, Simon *Kniha kódů a šifer: Tajná komunikace od starého Egypta po kvantovou kryptografii* Přeložili: Koubský, Petr - Eckhardtová, Dita. Praha: Dokořán, Argo, 2003. 382 s. ISBN: 80-86569-18-7; 80-7203-499-5

[3] Kahn, David *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* New York: Simon and Schuster, 1996. 1200 s. ISBN: 0-684-83130-9

[4] Vydavatelství Nová média, s. r. o. *Frekvenční analýza — Matematika.cz*[online]. c2006 Citováno dne 29.4.2015. <http://www.matematika.cz/frekvencni-analyza>

[5] Vydavatelství Nová média, s. r. o. *Friedmanův test — index koincidence — Matematika.cz*[online]. c2006 Citováno dne 29.4.2015. <http://www.matematika.cz/friedmanuv-test>

[6] Vydavatelství Nová média, s. r. o. *Odhadnutí délky klíče Vigenerovy šifry — Matematika.cz*[online]. c2006 Citováno dne 29.4.2015. <http://www.matematika.cz/kryptoanalyza-vigenerovy-sifry-2>

[7] Lyon, James *Practical Cryptography*[online]. c2009 - 2012 Citováno dne 29.4.2015. <http://practicalcryptography.com/ciphers/>

[8] Wikipedia.org *Kategorie:Klasické šifry – Wikipedie*[online]. c2014 Citováno dne 29.4.2015. <http://cs.wikipedia.org/wiki/Kategorie:Klasické_šifry>

[9] Wikipedia.org *http://en.wikipedia.org/wiki/Scytale*[online]. c2015 Citováno dne 29.4.2015 <http://en.wikipedia.org/wiki/Scytale>

[10] The History Blog *The History Blog & Blog Archive & An Enigma machine worth coveting*[online]. c2015 Citovnáno dne 29.4.2015 <http://www.thehistoryblog.com/archives/21186>

[11] Microsoft *ASCII Character Codes Chart 1*[online]. c2015 Citováno dne 29.4.2015 <https://msdn.microsoft.com/en-us/library/60ecse8t(v=vs.80).aspx>

A Popis uživatelského rozhraní

Popis demonstračního uživatelského rozhraní praktické části a návod jak postupovat při práci s ním.

A.1 Hlavní menu

Popis hlavního menu aplikace (viz obr. 8).

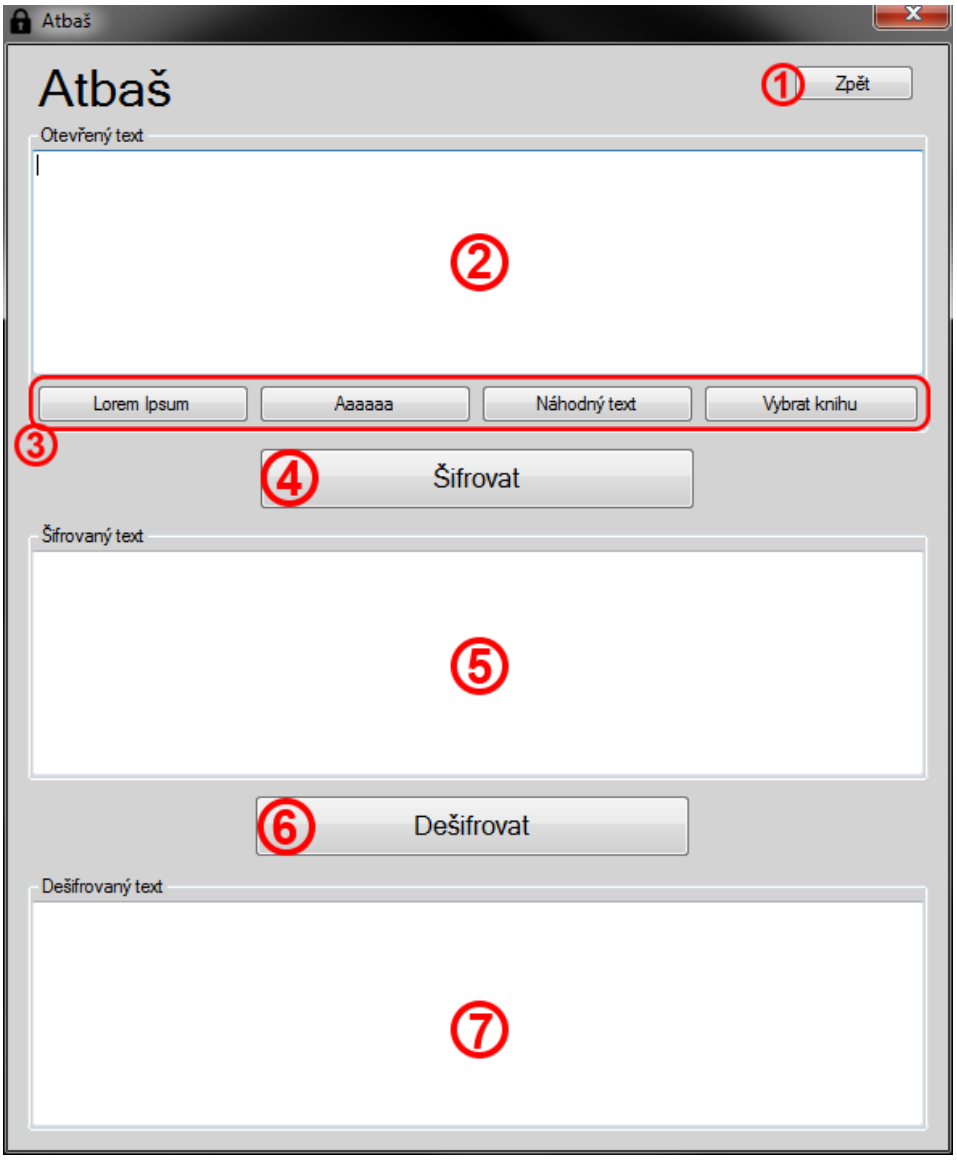
1. Otevře okno s šifrou Atbaš.
2. Otevře okno s Caesarovou šifrou.
3. Otevře okno s šifrou Enigma.
4. Otevře okno s šifrou Playfair.
5. Otevře okno s šifrou Rail Fence.
6. Otevře okno se Sloupcovou šifrou.
7. Otevře okno s jednoduchou substituční šifrou.
8. Otevře okno s Vernamovou šifrou.
9. Otevře okno s Vigenerovou šifrou.
10. Otevře okno pro analýzu textu.
11. Otevře okno pro prolomení Caesarovy šifry.
12. Otevře okno pro prolomení Vigenerovy šifry.

A.2 Šifra Atbaš

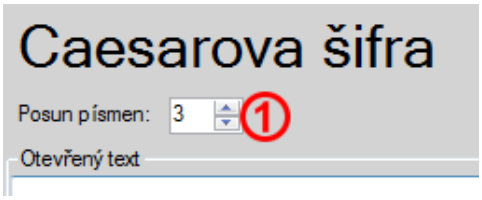
Popis okna s šifrou Atbaš (viz obr. 9). Nejdříve napíšeme text do pole pro otevřený text (2) nebo zvolíme jednu z možností připraveného textu (3). Poté zmáčkneme tlačítko šifrovat (4). Pro dešifrování se zmáčkne tlačítko dešifrovat (6).

1. Tlačítko pro přechod do předchozí nabídky.
2. Pole pro otevřený text.
3. Nabídka textu k vložení.
4. Tlačítko pro zašifrování otevřeného textu.
5. Pole pro zašifrovaný text.
6. Tlačítko pro dešifrování zašifrovaného textu.
7. Pole pro dešifrovaný text.

Obrázek 8: Hlavní menu aplikace



Obrázek 9: Okno pro šifrování šifrou Atbaš



Obrázek 10: Výřez okna pro šifrování Caesarovou šifrou

A.3 Caesarova šifra

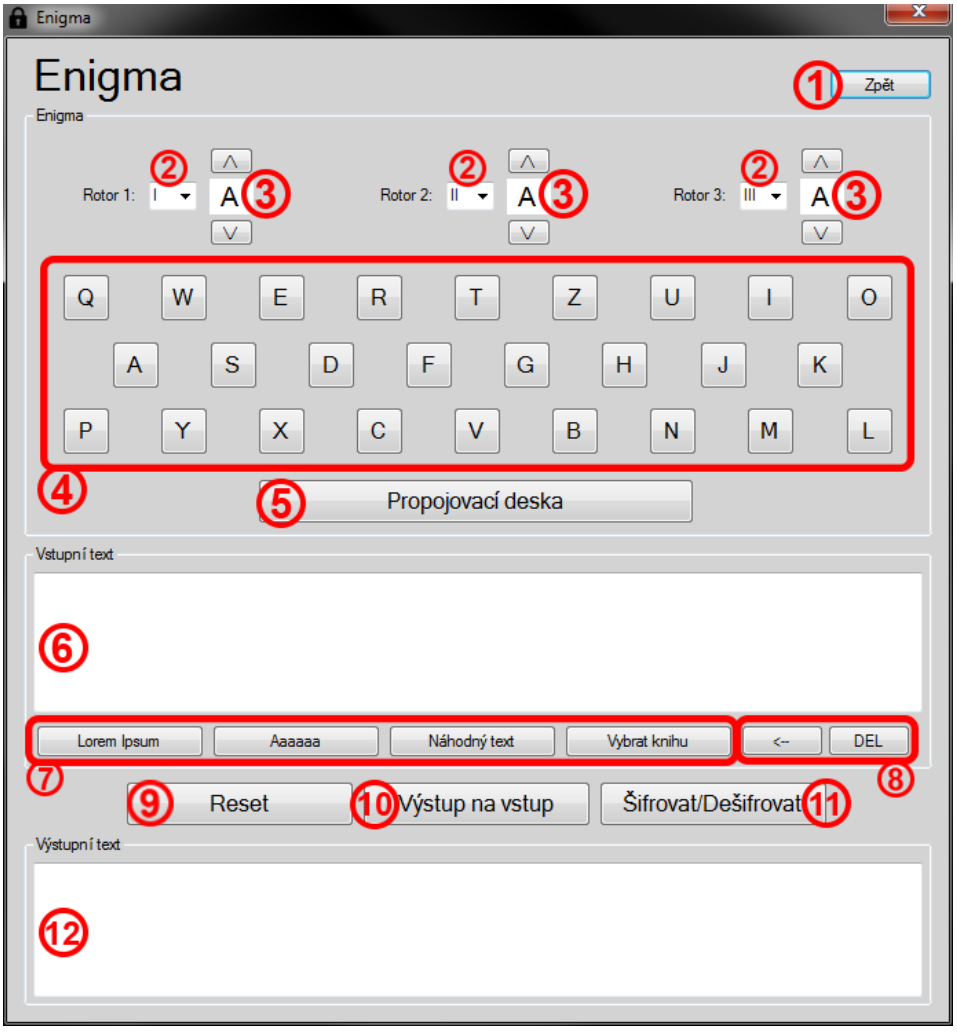
Popis okna s Caesarovou šifrou (viz obr. 10). Položkou (1) nastavujeme posun šifry. Práce s oknem je dále stejná jako u šifry Atbaš (viz sekce A.2).

1. Posun šifry.

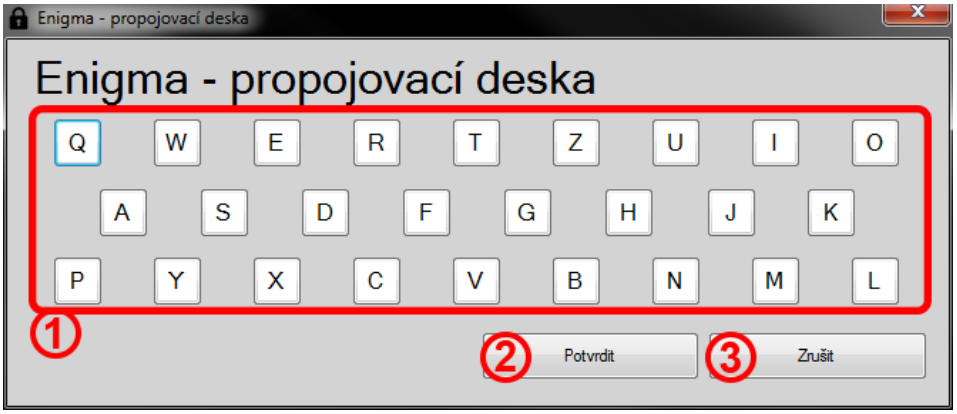
A.4 Enigma

Popis okna šifry Enigma (viz obr. 11). Před zahájením šifrování je nutné nastavit šifru. Můžeme nastavit typy rotorů (2), prvotní pootočení rotorů (3) a propojení na propojovací desce (viz obr. A.4) (5). Po zmáčknutí jakéhokoliv písmene na klávesnici (4), nebo po zmáčknutí tlačítka šifrovat/dešifrovat (11), se nastavení zamkne a začne se šifrovat. Nastavení lze odemknout tlačítkem reset (9). Pro dešifrování zašifrovaného textu z pole pro výstupní text (12) lze zmáčknut tlačítko výstup na vstup (10) a zašifrovaný text se překopíruje do pole pro vstupní text. Poté se pro dešifrování zmáčkne tlačítko šifrovat/-dešifrovat (11).

1. Tlačítko pro přechod do předchozí nabídky.
2. Položka pro nastavení typu rotoru.
3. Tlačítka pro nastavení posunu rotoru.
4. Klávesnice pro zadávání znaků.
5. Tlačítko pro přechod do okna propojovací desky.
6. Pole pro vstupní text.
7. Nabídka textu k vložení.
8. Smazání jednoho znaku, respektive celého textu.
9. Odemčení nastavení.
10. Tlačítko pro převedení výstupního textu na vstup.
11. Tlačítko pro manuální šifrování/dešifrování.
12. Pole pro výstupní text.



Obrázek 11: Okno pro šifrování Enigmou



Obrázek 12: Okno pro propojovací desku Enigmy

Propojovací deska Popis okna propojovací desky (viz obr. 12). Pro propojení písmen zmáčkněte tlačítko jednoho, to se označí, a pak dalšího. Propojení je znázorněné společnou barvou tlačítek. Pro zrušení propojení zmáčkněte libovolné tlačítko z dvojce jež se má rozpojit.

1. Písmena k propojení.
2. Potvrzení aktuálních změn propojení.
3. Zrušení aktuálních změn propojení.

A.5 Šifra Playfair

Popis okna s šifrou Playfair (viz obr. 13). Do pole (1) vepisujeme klíč šifry, podle kterého se bude tvořit Polybiova tabulka. Položkou (2) určujeme, které písmeno se bude nahrazovat písmenem (3). Práce s oknem je dále stejná jako u šifry Atbaš (viz sekce A.2).

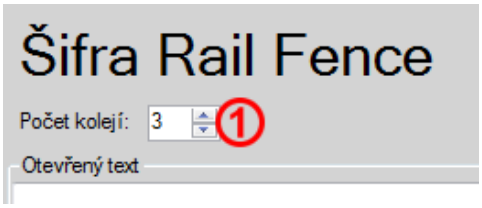
1. Položka pro vepsání klíče.
2. Znak který se nahrazuje.
3. Znak kterým nahrazujeme.

A.6 Šifra Rail Fence

Popis okna s šifrou Rail Fence (viz obr. 14). Položkou (1) nastavujeme počet kolejí šifry. Práce s oknem je dále stejná jako u šifry Atbaš (viz sekce A.2).

1. Počet kolejí šifry.

Obrázek 13: Výřez okna pro šifru Playfair



Obrázek 14: Výřez okna pro šifrování šifrou Rail Fence

A.7 Sloupcová šifra

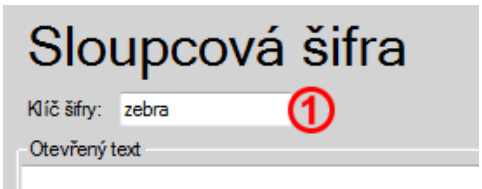
Popis okna s šifrou Rail Fence (viz obr. 15). Položkou (1) nastavujeme počet sloupců šifry. Práce s oknem je dále stejná jako u šifry Atbaš (viz sekce A.2).

1. Počet sloupců šifry.

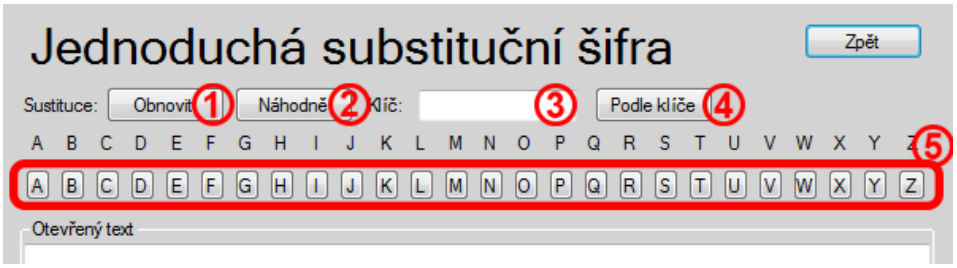
A.8 Jednoduchá substituční šifra

Popis okna s jednoduchou substituční šifrou (viz obr. 16). Tlačítky (5) lze nastavit jednotlivé substituce. Po zmáčknutí libovolného tlačítka s písmenem se toto tlačítko označí a po zmáčknutí dalšího se písmena vymění. Po vložení textového hesla (3) lze nastavit substituce dle tohoto hesla. Po zmáčknutí tlačítka (4) se vypíšou písmena hesla, každé jen jednou, a pak se doplní zbývající písmena podle abecedního pořadí. Tlačítkem obnovit (1) lze vrátit substituce do původní podoby. Práce s oknem je dále stejná jako u šifry Atbaš (viz sekce A.2).

1. Počet kolejí šifry.



Obrázek 15: Výřez okna pro šifrování sloupcovou šifrou



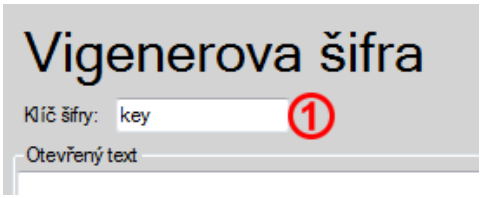
Obrázek 16: Výřez okna pro šifrování šifrou Rail Fence

Obrázek 17: Výřez okna pro šifrování Vernamovou šifrou

A.9 Vernamova šifra

Popis okna s Vernamovou šifrou (viz obr 17). Po vepsání nebo vložení otevřeného textu lze šifrovat. Pokud je položka (4) označena, po stisknutí tlačítka šifrovat (6) se klíč vygeneruje automaticky. Pokud není označena, musí se vygenerovat klíč tlačítkem generovat klíč (5). Práce s oknem je dále stejná jako u šifry Atbaš (viz sekce A.2).

1. Pole pro otevřený text.
2. Nabídka textu k vložení.
3. Pole s klíčem šifry.
4. Nabídka automatického nebo manuálního generování klíče.
5. Tlačítko pro generování náhodného klíče.
6. Tlačítko pro šifrování.



Obrázek 18: Výřez okna pro šifrování Vigenerovou šifrou

A.10 Vigenerova šifra

Popis okna s Vigenerovou šifrou (viz obr. 18). Položkou (1) nastavujeme klíč šifry. Práce s oknem je dále stejná jako u šifry Atbaš (viz sekce A.2).

1. Klíč šifry.

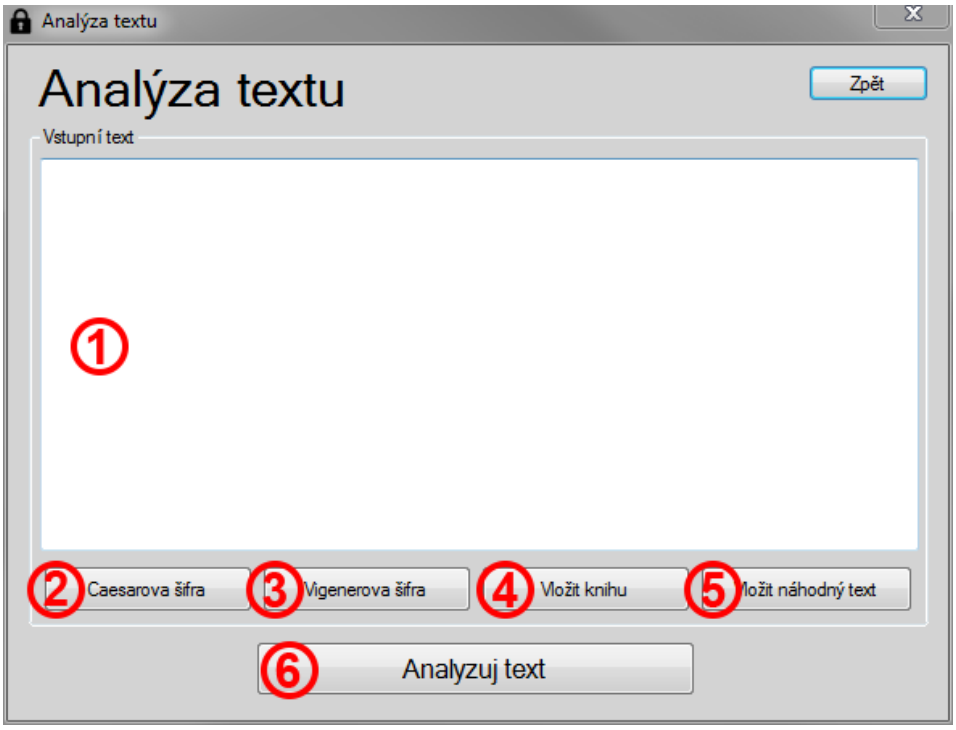
A.11 Analýza textu

Popis okna analýzy textu (viz obr. 19). Do pole pro vstupní text (1) můžete vepsat text, využít Caesarovy šifry (2), Vigenerovy šifry (3), vložit knihu (4) nebo vložit náhodný text. Poté zmáčkněte tlačítko *Analyzuj text* (6).

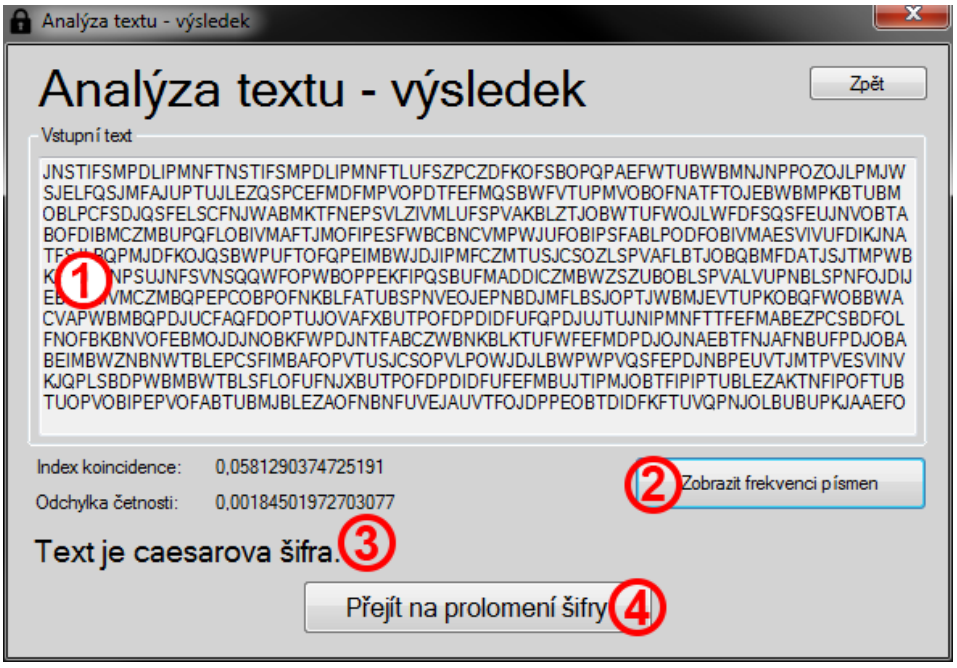
1. Pole s textem k analýze.
2. Tlačítko pro otevření okna s Caesarovou šifrou.
3. Tlačítko pro otevření okna s Vigenerovou šifrou.
4. Tlačítko pro vložení knihy.
5. Tlačítko pro vložení náhodného textu.
6. Tlačítko pro analyzování textu.

Analýza textu - výsledek Popis okna s výsledkem analýzy textu (viz obr. 20). Na této obrazovce se dozvíme výsledek analýzy (3). Můžeme si zobrazit okno s frekvencemi všech písmen (2) nebo přejít na dešifrování výsledné šifry (4).

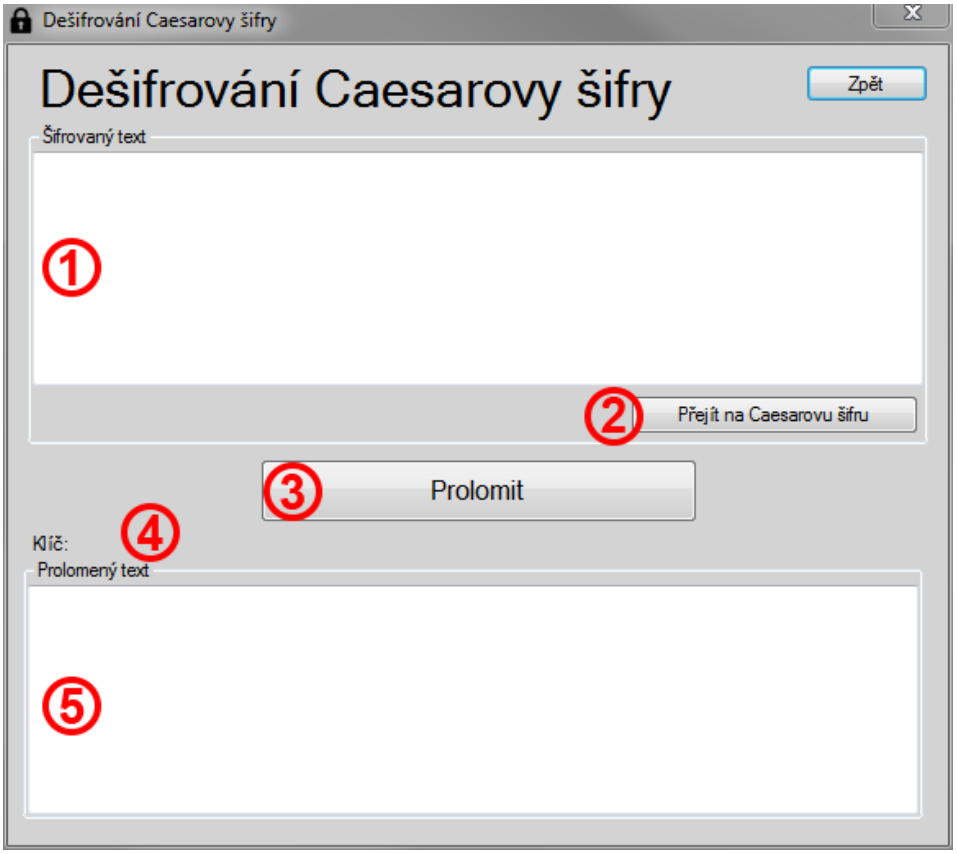
1. Pole pro zobrazení analyzovaného textu.
2. Tlačítko pro zobrazení frekvence jednotlivých písmen.
3. Výsledek analýzy.
4. Tlačítko pro přechod na dešifrování nebo tlačítko zpět.



Obrázek 19: Okno pro analýzu textu



Obrázek 20: Okno s výsledkem analýzy textu



Obrázek 21: Okno pro prolomení Caesarovy šifry

Prolomení Caesarovy šifry Popis okna k prolomení Caesarovy šifry (viz obr. 21). Můžeme vložit text zašifrovaný Caesarovou šifrou do pole (1) nebo tlačítkem (2) přejít na šifrování Caesarovou šifrou. Po vložení textu zmáčkneme tlačítko prolomit (3). Na pozici (4) se objeví klíč zašifrovaného textu a do pole (5) se vepíše text dešifrovaný podle zjištěného klíče.

1. Pole pro zašifrovaný text.
2. Tlačítko pro přechod na šifrování Caesarovou šifrou.
3. Tlačítko pro prolomení textu.
4. Pole s klíčem zašifrovaného textu.
5. Pole s dešifrovaným textem.

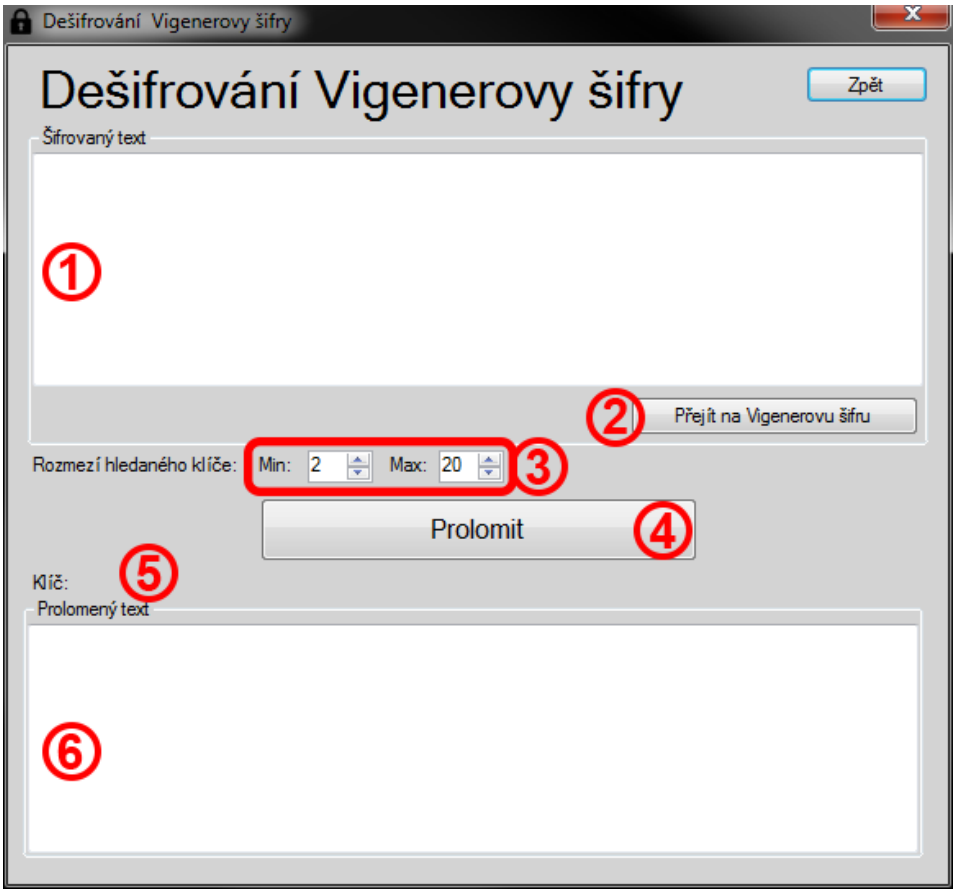
Prolomení Vigenerovy šifry Popis okna k prolomení Vigenerovy šifry (viz obr. 22). Můžeme vložit text zašifrovaný Vigenerovou šifrou do pole (1) nebo tlačítkem (2) přejít na šifrování Vigenerovou šifrou. Můžeme nastavit rozmezí délky hledaného klíče (3). Po vložení textu zmáčkneme tlačítko prolomit (4). Na pozici (5) se objeví klíč zašifrovaného textu a do pole (6) se vepíše text dešifrovaný podle zjištěného klíče.

1. Pole pro zašifrovaný text.
2. Tlačítko pro přechod na šifrování Vigenerovou šifrou.
3. Nabídka k nastavení minimální a maximální délky hledaného klíče.
4. Tlačítko pro prolomení textu.
5. Pole s klíčem zašifrovaného textu.
6. Pole s dešifrovaným textem.

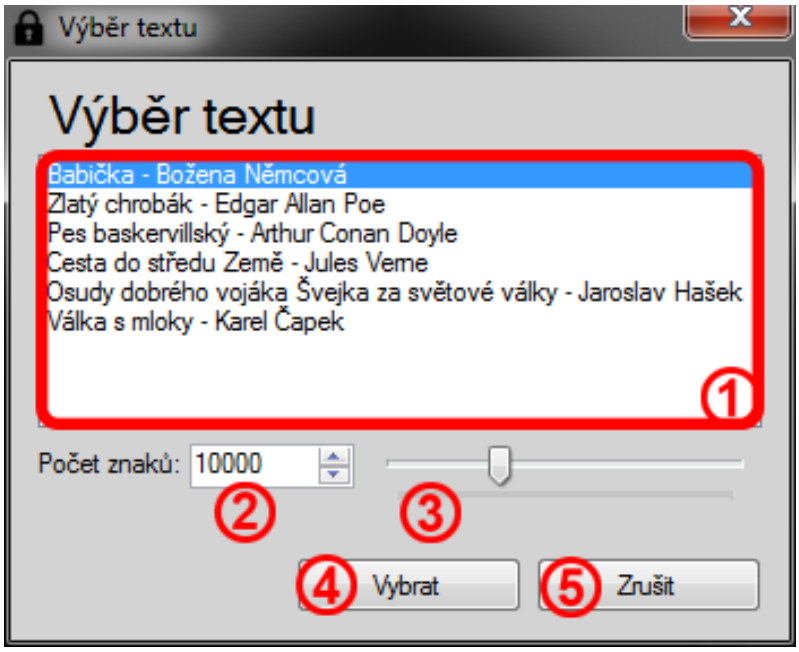
A.12 Výběr knihy

Popis pomocného okna s výběrem textu z knihy (viz obr. 23). Ze seznamu (1) vybereme knihu a označíme. Položkami (2) a (3) můžeme určit délku vybraného textu. Tlačítkem vybrat (4) zkopírujeme text anebo tlačítkem zrušit (5) ukončíme výběr bez kopírování.

1. Seznam knih k výběru.
2. Nastavení délky výběru textu.
3. Nastavení délky výběru textu.
4. Potvrzení výběru.
5. Zrušení výběru.



Obrázek 22: Okno pro prolomení Vigenerovy šifry



Obrázek 23: Okno s výběrem textu z knihy